1

INTRODUZIONE

Il progetto e la realizzazione di un moderno impianto di elaborazione si basano sempre di più sul concetto di *rete*. Le reti di calcolatori sono nate negli anni sessanta come veicolo con cui collegare terminali periferici ad elaboratori centrali, i mainframe. Di anno in anno sono diventate sempre più importanti, ma soltanto con la comparsa dell'informatica individuale, e cioè dei personal computer e delle workstation, hanno assunto un ruolo insostituibile. Infatti, un insieme di personal computer e workstation, anche se molto potenti, non può da solo rimpiazzare un mainframe, in quanto questo è anche il luogo dove gli utenti del sistema informativo condividono le informazioni e le risorse hardware e software. Si consideri il classico sistema di prenotazione aerea: le informazioni sui voli e sui posti prenotati sono condivise da tutti gli utenti del sistema tramite la base di dati presente sul mainframe stesso. Un insieme di piccole basi di dati, localizzate su singoli personal computer, non produrrebbe lo stesso risultato.

L'informatica personale, con potenza di calcolo distribuita nei singoli posti di lavoro, diventa competitiva rispetto a quella centralizzata basata su un mainframe soltanto se i personal computer e le workstation sono interconnessi da un'idonea rete di calcolatori. È la rete di calcolatori che diventa il veicolo di condivisione dell'informazione e permette quindi di sostituire al mainframe e ai suoi terminali "stupidi" una moltitudine di piccoli elaboratori "intelligenti", opportunamente interconnessi tra loro. È questa la rivoluzione più importante che l'informatica sta affrontando e che prende il nome di *downsizing*.

Affinché ciò avvenga i problemi tecnici da affrontare sono molti. Per prima cosa occorre considerare che i sistemi informativi non sono entità statiche: essi infatti si devono adattare rapidamente alla continua evoluzione delle realtà in cui sono inseriti. Si pensi alle aziende che vengono ogni giorno acquistate, fuse, trasformate, cedute: i loro sistemi informativi devono seguire sorti simili. Si pensi poi ai sistemi informativi per le amministrazioni pubbliche e private che devono ogni giorno adattarsi ai cambiamenti legislativi.

VISIT…

Quindi i sistemi informativi stessi devono essere estremamente flessibili ed in particolare devono esserlo le reti di calcolatori che ne sono la spina dorsale. Recentemente si parla spesso di autostrade elettroniche, cioè di sistemi di telecomunicazioni ad altissima velocità in grado di veicolare informazioni di qualsiasi tipo: proprio queste autostrade elettroniche dovrebbero fungere da elemento trasmissivo portante per le reti di calcolatori aziendali ed interaziendali del futuro.

1.1 CARATTERISTICHE DI UNA RETE DI CALCOLATORI

Abbiamo già detto che lo scopo principale delle reti di calcolatori è la condivisione dell'informazione e delle risorse hardware e software. Creiamo reti di calcolatori perché i loro utenti possano condividere programmi, dati, dispositivi periferici, indipendentemente dalla loro collocazione fisica. Questa struttura è effettivamente concorrenziale rispetto al mainframe perché presenta i seguenti vantaggi:

Alta affidabilità

Con una rete di calcolatori è possibile disporre di risorse alternative in caso di necessità. Infatti i singoli componenti hanno costi contenuti ed ogni azienda può avere a disposizione parti sostitutive senza immobilizzare grandi capitali. Rendere affidabile un mainframe costa molto di più che rendere affidabile una rete di piccoli calcolatori.

Risparmio

Non vi è dubbio che i costi dell'hardware e del software per realizzare un sistema distribuito sono di un ordine di grandezza inferiori a quelli per realizzare un sistema centralizzato basato su mainframe. L'unico aspetto negativo è legato all'impossibilità di trasportare facilmente un software scritto per un sistema centralizzato su un sistema distribuito: è indispensabile una ricodifica con tecniche più moderne, ma, d'altro canto, si ottiene un prodotto con caratteristiche estremamente superiori. Non deve infine essere trascurato il problema dell'istruzione permanente degli analisti, dei programmatori e degli utenti verso queste nuove tecnologie.

Gradualità della crescita

Dopo che l'infrastruttura di rete è stata creata, l'aggiunta di nuove potenzialità, ove servono, è semplice e poco costosa. Si possono aggiungere un posto di lavoro o attivare nuovi servizi o potenziare i server esistenti senza interruzioni di servizio e con costi dilazionati nel tempo.

1.2 TIPI DI RETI

La tabella 1.1 riporta una tassonomia dei vari tipi di rete, in funzione dell'ambito operativo e delle distanze coperte.

Il primo gruppo di reti si utilizza per l'interconnessione di più processori all'interno dello stesso calcolatore (calcolatori paralleli) ed esula dalla trattazione fatta in questo testo. Il secondo gruppo prende il nome di reti di calcolatori e riguarda l'interconnessione di elaboratori eterogenei.

	Ambito	Distanza	Rete
Calcolatori paralleli	Circuito stampato	0.1 m	Massive Parallel
	Sistema	1 m	Multi Processor
	Stanza	10 m	Cluster
Reti di Calcolatori	Edificio	100 m	Reti Locali
	Comprensorio	1 km	Reti Locali Estese
	Città	10 km	Reti Metropolitane
	Nazione	100 km	Reti Geografiche
	Continente	1000 km	Reti Geografiche
	Pianeta	10000 km	Reti Geografiche

Tab. 1.1 - Tipi di reti.

1.3 ASPETTI PROGETTUALI

Il progetto di una rete di calcolatori deve considerare, ai fini della flessibilità, diversi importanti aspetti:

- Le architetture proprietarie. Esistono oggi molte reti proprietarie che hanno grande diffusione a livello nazionale e internazionale e che non possono certamente essere ignorate anche se non sono assolutamente standard. Esse sono progettate in base a scelte indipendenti ed arbitrarie dei costruttori. Esempi sono IBM/SNA, Digital/DECnet-IV e Novell/IPX.
- Gli standard "de facto". Un esempio estremamente significativo è il TCP/IP, sistema di rete a larghissima diffusione non riconosciuto da nessun organismo internazionale di standardizzazione. Un altro esempio è Ethernet v.2.0, che è oggi la rete locale più diffusa, spesso confusa con IEEE 802.3.
- Gli standard "de iure", emessi dall'ISO (International Standard Organization)

e dal CCITT (Comité Consultatif International de Telegraphie et Telephonie). Tra questi spiccano il progetto IEEE/ISO 802 (per le reti locali) e l'OSI (Open Systems Interconnection).

- L'evoluzione tecnologica. Essa non può certo essere fermata in attesa che gli enti di standardizzazione abbiano completato il loro lavoro. Ad esempio, per definire lo standard ATM (Asynchronous Transfer Mode), le ditte realizzatrici di prodotti si sono riunite in un consorzio (ATM Forum) i cui lavori per le proposte di standardizzazione procedono molto più speditamente di quelli del CCITT.

1.4 LA STRUTTURA DI UNA RETE DI CALCOLATORI

Scopo di questo libro è spiegare quale può essere l'organizzazione di una rete di calcolatori di tipo *corporate* e *multiprotocol*.

- *Corporate* perché una rete di calcolatori deve servire l'intera azienda in tutte le sue funzioni (per esempio dalla progettazione alle vendite) e in tutte le sue sedi eventualmente distribuite sul territorio. Inoltre, tale rete deve essere collegata efficientemente con le reti di aziende appartenenti alla stessa holding o che hanno con essa frequenti rapporti interaziendali.
- *Multiprotocol* perché è illusorio pensare di riuscire ad imporre all'interno di una azienda un'unica architettura di rete. Infatti occorre considerare che le reti sono nate all'interno delle aziende non con un progesso progettuale "top-down", bensì con un'integrazione di tipo "bottom-up" in cui reti diverse, eterogenee, nate per risolvere problemi specifici, sono state a poco a poco integrate per formare una rete aziendale. Tale situazione si complica ulteriormente tutte le volte che si verificano fusioni interaziendali in cui occorre fondere anche sistemi informativi eterogenei.

In letteratura tale problema è anche noto con il termine *internetworking*. Questo testo vorrebbe avere un respiro un po' più ampio, insegnando prima a progettare e a realizzare le varie componenti di una rete di calcolatori e poi ad interconnetterle tra loro.

La figura 1.1 riporta la struttura di una rete di calcolatori di una ipotetica azienda. Essa è formata da una rete locale (LAN: Local Area Network) in ogni sede (edificio) dell'azienda; le LAN presenti all'interno di un'area metropolitana sono collegate tra di loro tramite MAN (Metropolitan Area Network) e queste a loro volta tramite una rete geografica (WAN: Wide Area Network). Occorre notare che oggi la diffusione delle MAN è limitata e i loro compiti sono spesso affidati alle WAN.

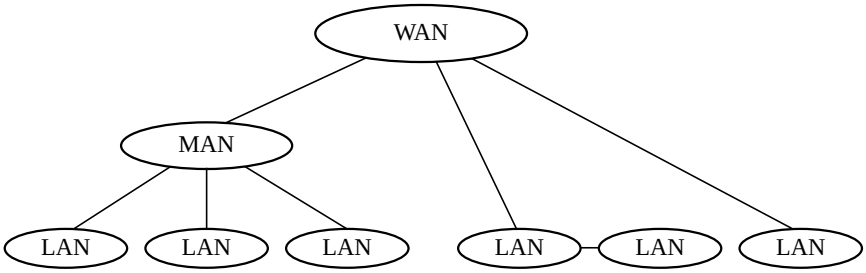


Fig. 1.1 - Esempio di interconnessione di reti.

1.5 GLI STANDARD

Il compito di progettare e gestire una "corporate mutiprotocol network" può sembrare immane, e in parte lo è, anche se oggi gli standard sia de iure che de facto ci vengono in aiuto. In questa introduzione è bene ricordare quali sono gli enti pubblici e privati di standardizzazione che si occupano di reti di calcolatori e quindi quali sono i principali standard.

1.5.1 "Chi è chi" nel mondo degli standard

- PTT *(Post, Telegraph & Telephone)* è l'amministrazione che gestisce in una nazione i servizi trasmissivi (in Italia il Ministero delle Poste e delle Telecomunicazioni);
- CCITT *(Comité Consultatif International de Telegraphie et Telephonie)* è l'organismo internazionale che emette le specifiche tecniche che devono essere adottate dalle PTT. È recentemente entrato a far parte dell'ITU (*International Telecommunication Union*).
- ISO *(International Standard Organization)* è il principale ente di standardizzazione internazionale che si occupa anche di reti di calcolatori.
- ANSI *(American National Standards Institute)* è il rappresentante USA nell'ISO.
- UNINFO è il rappresentante italiano nell'ISO per le tematiche di reti di calcolatori.
- IEEE *(Institute of Electrical and Electronics Engineers)* è l'organizzazione professionale mondiale degli ingegneri elettrici ed elettronici con gruppi di standardizzazione sulle reti di calcolatori.

1.5.2 L'OSI (Open Systems Interconnections)

L'OSI è un progetto di ampio respiro formulato dall'ISO alla fine degli anni '70 con lo scopo principale di fungere da *modello di riferimento* per le reti di calcolatori. Esso, infatti, doveva servire come base comune per coordinare gli sforzi dei vari sviluppatori, ad esempio standardizzando la terminologia e definendo quali sono le funzionalità di una rete. Per gestire la complessità dei problemi, l'OSI ha adottato un approccio a livelli (*layers*): l'intero problema della comunicazione tra due applicazioni è stato spezzato in un insieme di sette livelli, ciascuno dei quali esegue funzioni ben specifiche. OSI ha avuto inoltre il merito di fungere più in generale da elemento di coordinamento tra tutte le attività di standardizzazione, scopo che è stato senza dubbio raggiunto.

Tuttavia OSI si prefigge di essere molto più di un importante modello di riferimento. Infatti l'ISO ha standardizzato per OSI una serie di *protocolli*, da inserirsi ai vari livelli del modello, per formare una vera e propria architettura di rete concorrenziale con altre quali SNA, DECnet o TCP/IP.

Nel processo di standardizzazione, OSI è partito dai livelli bassi (quelli più vicini all'hardware) ed è salito verso quelli alti (quelli più vicini all'uomo) ricevendo gradimento ed accettazione differenti. I livelli 1 (Fisico) e 2 (Data Link) di OSI sono oggi assolutamente standard e questo consente l'interoperabilità dei prodotti. Dal livello 3 al livello 7 i protocolli esistono da tempo, ma hanno difficoltà ad imporsi per l'alto impatto che la loro adozione ha sul software dei sistemi informativi stessi e sui dispositivi di instradamento (router). Solo la Digital Equipment Corp. ha deciso di abbandonare la propria architettura di rete proprietaria (DECnet fase IV) a favore di un'architettura totalmente OSI (DECnet fase V).

1.5.3 Il progetto IEEE 802

Tale progetto, perfettamente inserito nel modello OSI, riguarda i livelli 1 e 2 limitatamente alle reti locali e metropolitane. Concepito anch'esso tra la fine degli anni '70 e l'inizio degli anni '80, ha portato ad una voluminosa serie di standard noti con sigle del tipo 802.X, oggi anche approvati dall'ISO. IEEE 802 è nato per razionalizzare i numerosi sforzi presenti in quegli anni per la creazione di nuove reti locali, spesso appositamente concepite - per ragioni commerciali - per essere incompatibili una con l'altra, ed ha ottenuto un notevole successo. Acquistare oggi una scheda di rete locale compatibile con uno standard 802 è certezza di buon investimento.

1.5.4 Gli standard CCITT

L'ISO non può affrontare autonomamente il problema della standardizzazione dei livelli 1 e 2 del modello OSI per le reti geografiche. A tal scopo si appoggia al CCITT che a livello 1 utilizza standard consolidati quali RS-232 (o gli equivalenti V.24 e V.28), V.35 e G.703/704, mentre a livello 2 adotta una famiglia di standard derivati dal protocollo SDLC (Synchronous Data Link Control) proposto da IBM per la rete SNA. SDLC stesso non viene riconosciuto come standard, ma alcune sue importanti varianti sì, quali HDLC, LAP-B, LAP-D e LAP-F. Inoltre, una variante di HDLC denominata LLC (Logical Link Control) viene adottata dall'IEEE per le reti locali con la sigla 802.2.

1.6 IL CABLAGGIO STRUTTURATO DEGLI EDIFICI

L'ingegneria civile ha da lungo tempo incluso nel progetto della costruzione o ristrutturazione degli edifici una parte impiantistica. Esistono norme su come realizzare la distribuzione elettrica, gli impianti idraulici, gli impianti telefonici, ecc., ma ancora oggi vengono spesso trascurati gli impianti per la "trasmissione dei segnali" (TV, citofonia, dati digitali, ecc.). Di questi, i più importanti in ambiente industriale e commerciale sono quelli per la trasmissione dei dati digitali. Essi sono nati come strutture stellari rispetto al mainframe, spesso in cavo coassiale. L'avvento delle reti locali modificò tali cablaggi che comunque rimasero dedicati a fungere da mezzo fisico per le reti di calcolatori. Inoltre, tali impianti non venivano quasi mai compresi nel capitolato dei lavori di realizzazione o ristrutturazione degli edifici e quindi erano sempre realizzati successivamente (su edifici già ultimati) con risultati discutibili a causa della necessità di attraversare quasi ogni vano con numerosi cavi.

Negli anni '80 ci si è orientati verso l'adozione di centralini telefonici digitali (PABX) come mezzo con cui trasportare le reti di calcolatori, con risultati molto scadenti, come discusso nel paragrafo 5.1.3. Gli anni '90 sono stati caratterizzati dalla comparsa di standard quali l'EIA/TIA 568 e 569 e il successivo ISO/IEC 11801 sul cablaggio strutturato degli edifici. Tali standard regolamentano la progettazione e realizzazione degli impianti per il trasporto dei segnali da effettuarsi contestualmente alla costruzione o alla ristrutturazione organica di un edificio. Sul cablaggio strutturato si veicolano molte informazioni di natura diversa: le LAN, la telefonia classica e numerica (ISDN), gli allarmi, i controlli e le regolazioni, le immagini video, il controllo presenze, ecc. Quando oltre alla struttura di cablaggio sono presenti elaboratori e software appositi dedicati al controllo dell'edificio allora si parla di *edifici intelligenti*.

1.7 I MEZZI TRASMISSIVI

Grazie alle recenti innovazioni tecnologiche, i mezzi trasmissivi attualmente utilizzati per le reti locali sono soltanto più due, la fibra ottica e il doppino di rame, e il cavo coassiale è stato quasi del tutto abbandonato.

La tecnologia per la produzione della fibra ottica è un sottoprodotto di quella per la purificazione del silicio sviluppata per la costruzione dei circuiti integrati. La fibra ottica è un mezzo trasmissivo quasi ideale: altissima banda, bassissima attenuazione, totale immunità ai disturbi elettromagnetici. Purtroppo il costo della connettorizzazione ne limita ancora molto l'utilizzo su larga scala. Essa è praticamente sempre adottata per la realizzazione di dorsali (interconnessione di reti), ma trova difficoltà ad imporsi come mezzo trasmissivo per il cablaggio fino alla stazione utente. Per quest'ultima applicazione si usa il doppino in rame che ha beneficiato negli ultimi anni di incredibili miglioramenti tecnologici. Nato per trasportare la telefonia in banda base (con spettro del segnale dell'ordine di 3 KHz), è stato migliorato e ingegnerizzato sino a poter trasportare segnali a frequenze dell'ordine delle centinaia di MHz. Ridotti costi, semplice connettorizzazione, facilità di posa, naturale compatibilità con la telefonia sono le sue caratteristiche vincenti. Oggi è acceso il dibattito se il doppino di rame debba essere schermato oppure no e di questo parleremo nei capitoli 3 e 4.

1.8 LE RETI LOCALI

Il cablaggio strutturato è il veicolo preferenziale per il trasporto dei dati delle reti locali (LAN). Accanto alle due reti locali "storiche" Ethernet e Token Ring si sono oggi aggiunte tutte quelle comprese nel progetto IEEE 802 e altre ancora che sono state standardizzate da altri enti (ad esempio l'ANSI ha standardizzato FDDI).

Una rete locale è un mezzo di trasporto equamente condiviso tra tutte le stazioni che vi si collegano, ad alta velocità e basso tasso di errore, limitato ad un ambito locale (senza attraversamento di suolo pubblico). Dato che l'estensione è limitata a comprensori privati, le LAN non necessitano di essere conformi agli standard CCITT.

Le velocità trasmissive sono comprese nell'intervallo 4 Mb/s - 100 Mb/s. Il mercato delle medie prestazioni è ormai dominato da IEEE 802.3 (evoluzione di Ethernet), mentre quello delle alte prestazioni è in grande fermento per i molti contendenti: FDDI, Ethernet a 100 Mb/s e ATM. Tutte queste reti adottano come mezzo trasmissivo preferenziale il doppino di rame e la fibra ottica per le dorsali.

1.9 LE RETI METROPOLITANE

Nate dallo sforzo di standardizzazione congiunto tra ISO e CCITT, sono estensioni delle reti locali in ambito urbano. All'interno di una città, infatti, le PTT dispongono spesso di dorsali in fibra ottica, veloci ed affidabili. Le prestazioni classiche raggiunte sono comprese tra i 2 Mb/s e i 140 Mb/s.

1.10 LE RETI GEOGRAFICHE

Le reti geografiche si basano sui servizi offerti dal fornitore nazionale di telecomunicazioni. In Italia, ad esempio, la trasmissione dati è nata con i CDA (Canali Diretti Analogici) i quali sono stati sostituiti nel tempo con i CDN (Canali Diretti Numerici) forniti dalla Telecom Italia. Le velocità di tali canali attualmente variano dai 2400 b/s ai 2 Mb/s. Sono inoltre state realizzate reti pubbliche per la sola trasmissione dei dati quali quelle conformi allo standard X.25 (in Italia ITAPAC).

Grazie anche alla liberalizzazione del mercato delle telecomunicazioni stanno comparendo nuove offerte di rete pubblica (WAN e MAN). Tra queste ricordiamo Frame-Relay, SMDS (Switched Multi-Megabit Data Service) e ATM (Asynchronous Transfer Mode), che sono concepite per trasmissione dati a velocità rispettivamente medie (64 Kb/s-2 Mb/s), alte (2 Mb/s-34 Mb/s) e altissime (155 Mb/s e oltre).

1.11 L'INTERNETWORKING

La struttura di rete corporate e multiprotocol precedentemente descritta implica problematiche di *internetworking* tutte le volte che ci si trova a collegare due LAN tra di loro, una LAN con una MAN, una LAN con una WAN, ecc. L'internetworking, a causa dell'eterogeneità delle architetture di rete già citate, deve essere necessariamente *multiprotocollo*. Questo significa che la stessa struttura fisica, sia locale sia geografica, deve essere utilizzata simultaneamente da più architetture di rete (SNA, DECnet, TCP/IP, ecc.) le quali devono convivere il più armoniosamente possibile. In generale, è opportuno cercare di minimizzare gli investimenti creando sinergie tra tutte le strutture atte a trasportare informazione. Ad esempio, a livello di rete geografica si cerca sempre più di far convivere sugli stessi mezzi trasmissivi non solo i vari protocolli delle reti di calcolatori, ma anche le comunicazioni telefoniche e le videoconferenze tra sedi distinte della stessa azienda. All'interno degli edifici tale problema è così sentito che sono nati i già citati standard che specificano come

realizzare i cablaggi.

La convivenza di più protocolli diversi è una realtà presente a vari livelli del modello OSI. Una prima forma si ha a livello di cablaggio strutturato: mezzi trasmissivi generici (doppini e fibre) possono essere utilizzati per trasportare diversi standard di rete locale (Ethernet, FDDI, ecc.).

Una seconda soluzione, che è probabilmente la più interessante, è quella di far convivere più architetture di rete sulla stessa rete locale: ad esempio, una rete Token Ring può trasportare contemporaneamente i protocolli TCP/IP e OSI. Tale supporto multiprotocollo è ormai standard da tempo sulle LAN grazie all'adozione del già menzionato LLC (802.2), ma diventa problematico quando lo si debba estendere alla rete geografica. Per questo sono nati i bridge/router multiprotocollo (spesso detti brouter) in grado di fornire tale supporto sia sulla rete locale che su quella geografica.

Una terza forma di convivenza di protocolli diversi si ha quando su un protocollo di livello 3 si appoggiano più pile di protocolli di livello superiore: in DECnet fase V, ad esempio, sul livello 3 OSI si appoggiano sia la pila di protocolli OSI (per fornire applicativi quali X.400, FTAM, X.500) sia la pila di protocolli DECnet fase IV (a partire dal protocollo di livello 4 in su) per garantire l'utilizzabilità di tutti i classici applicativi DECnet.

1.12 I SISTEMI OPERATIVI DI RETE

Le reti di calcolatori sarebbero di poca utilità se non fossero corredate da una grande varietà di software. In particolare, se si vogliono realizzare dei sistemi distribuiti di basso costo concorrenziali ai mainframe (il downsizing di cui si è parlato precedentemente) è necessario che il software operi sulle piattaforme utilizzate (ad esempio personal computer e workstation), congiuntamente ai sistemi operativi più diffusi: MS-DOS, Microsoft Windows, Unix e Macintosh. Sono nate a tal scopo apposite architetture di rete, spesso dette anche *sistemi operativi di rete,* per risolvere i problemi di downsizing prima citati. Un primo gruppo prende il nome di sistemi *peer-to-peer* e comprende, ad esempio, Windows for Workgroup e Novell Lite; un secondo gruppo, con funzionalità più sofisticate, prende il nome di *client-server* e comprende, ad esempio, Novell Netware, Microsoft LAN Manager e Banyan Vines. Queste due classi di sistemi offrono sostanzialmente le stesse funzionalità, ma i primi sono indicati per ambienti di dimensioni ridotte, mentre i secondi possono collegare migliaia di client e decine di server e fornire le interfacce verso altre architetture.

1.13 GLI APPLICATIVI

Gli applicativi di rete sono quei programmi che scambiano informazioni utilizzando la rete. Le tre applicazioni per cui le reti sono storicamente nate sono il terminale virtuale, il trasferimento di file e la posta elettronica. Accanto a queste tre applicazioni, oggi sono disponibili numerose altre quali l'accesso a banche dati, la ricerca e il trasferimento di dati e programmi, lo scambio di documenti con validità legale, le bacheche elettroniche, la localizzazione di utenti sulla rete, ecc.

Tali applicativi, grazie anche all'adozione di interfacce grafiche e a finestre, sono diventati facili da usare anche per utenti inesperti e hanno contribuito enormemente alla diffusione delle reti stesse.

BIBLIOGRAFIA

[1] A. Tanenbaum, "Computer Networks", Prentice-Hall.

[2] W. Stalling, "Data and Computer Communication", Macmillan.

2

IL MODELLO ISO/OSI

Alla fine degli anni '70, l'ISO sentì la necessità di proporre una serie di standard per le reti di calcolatori e avviò il Progetto OSI (Open System Interconnection), uno standard che propose un modello di riferimento per l'interconnessione di sistemi aperti. Il documento principale che illustra tale attività è il *Basic Reference Model* di OSI, standard ISO 7498 [1].

2.1 IL MODELLO DI RIFERIMENTO OSI

Il modello di riferimento OSI ha due scopi:

- fornire una base comune su cui sviluppare standard per l'interconnessione di sistemi informatici;
- fornire un modello rispetto a cui confrontare le architetture di rete proprietarie.

Il modello di riferimento OSI non ha come scopo la definizione di servizi o protocolli specifici. A questo sono stati delegati altri enti (es. IEEE, CCITT) o l'ISO stessa, in tempi successivi.

2.2 SISTEMI, APPLICAZIONI E MEZZI TRASMISSIVI

OSI introduce il concetto di *sistema (system)* come un insieme di uno o più elaboratori con il relativo software, periferiche, terminali, operatori umani, processi, ecc. che complessivamente è in grado di elaborare dati. Nell'ambito di un sistema un'*applicazione (application)* è l'elemento che effettivamente svolge l'elaborazione dei dati.

Lo standard OSI tratta lo scambio di informazioni tra i sistemi e non come i sistemi sono realizzati o funzionano al loro interno. Tale trasferimento di informazioni avviene su *mezzi fisici (physical media)* secondo lo schema riportato in figura 2.1.

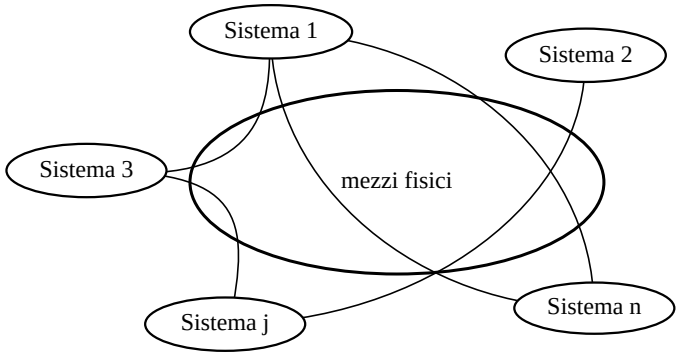


Fig. 2.1 - Sistemi interconnessi da mezzi fisici.

L'architettura del modello di riferimento OSI è stata progettata pensando a tre componenti principali:

- il processo applicativo che deve scambiare le informazioni;
- la connessione che permette lo scambio delle informazioni;
- i sistemi.

Un esempio è illustrato in figura 2.2.

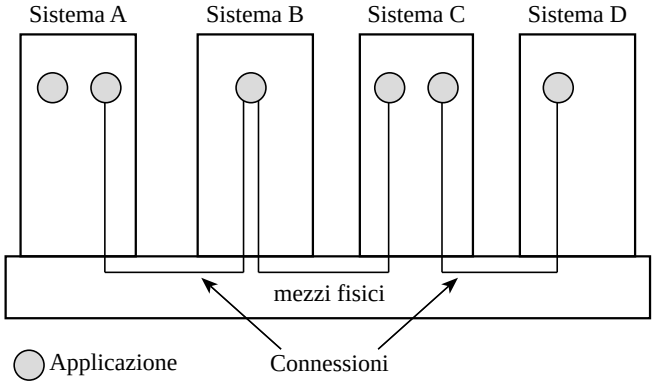


Fig. 2.2 - Elementi Base di OSI.

2.3 ARCHITETTURA A LIVELLI

Per ridurre la complessità progettuale, OSI introduce *un'architettura a livelli (layered architecture)* i cui componenti principali sono:

- i livelli (*layers*);
- le entità (*entities*);
- i punti di accesso al servizio (SAP: *Service Access Points*);
- le connessioni (*connections*).

In una tale architettura, ciascun sistema è decomposto in un insieme ordinato di livelli, rappresentati per convenienza come una pila verticale. In figura 2.3 sono rappresentati i livelli che compongono il modello di riferimento ISO-OSI.

Fig. 2.3 - Il modello ISO/OSI.

Livelli adiacenti comunicano tramite la loro *interfaccia* (*interface*). Ogni livello è poi composto da una o più *entità*. Entità appartenenti allo stesso livello, su sistemi diversi, vengono dette *peer-entities.*

Tale approccio di progettazione a livelli è comune a tutte le moderne architetture di rete; ciò che varia dall'una all'altra è il numero dei livelli, il loro nome e le entità contenute.

Lo scopo di ciascun livello è quello di fornire servizi alle entità del livello superiore, mascherando il modo in cui questi sono implementati. Ad eccezione del livello più alto, un livello N fornisce servizi di livello N alle entità di livello N+1.

Le entità di livello N, eccetto il livello 1, per comunicare usano servizi di livello N - 1. Le entità di livello 1 comunicano direttamente tramite i mezzi trasmissivi che le interconnettono.

Le entità usano e forniscono servizi tramite i SAP (Service Access Points), come illustrato in figura 2.4.

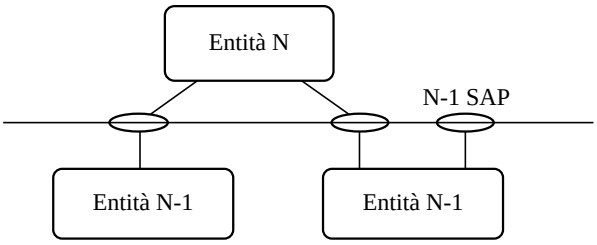


Fig. 2.4 - Entità e SAP.

Le operazioni specifiche di un livello, cioè la cooperazione tra le entità appartenenti a quel livello, sono realizzate da un insieme di *protocolli (protocol).* Affinché due entità di livello N su sistemi diversi possano scambiarsi informazioni, una connessione deve essere stabilita nel livello N-1 usando un protocollo di livello N-1. Tale connessione di livello N-1 è stabilita tra due SAP di livello N-1.

2.4 PROTOCOLLI, LIVELLI E INTERFACCE

Riassumendo, livelli N comunicano attraverso un protocollo di livello N: ogni livello deve quindi mostrare un'interfaccia ben definita a quello immediatamente superiore, come viene mostrato in figura 2.5.

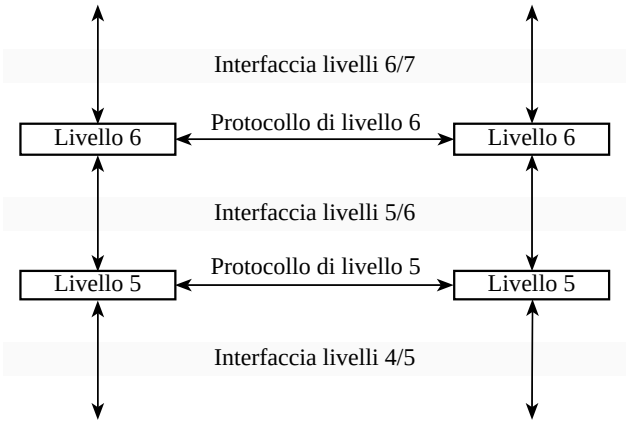


Fig. 2.5 - Livelli, protocolli e interfacce.

Anche se è definito un protocollo di livello N, nessun dato è trasferito direttamente da un livello N all'altro; infatti ogni livello passa dati e informazioni di controllo a quello sottostante, sino a quando si giunge al livello Fisico, che effettua la trasmissione. L'interfaccia definisce quali operazioni primitive e quali servizi sono forniti da un livello ai livelli superiori.

2.5 PRINCIPALI ARCHITETTURE DI RETE

L'insieme dei livelli, dei protocolli e delle interfacce definisce un'architettura di rete. Le architetture di rete più note sono:

- SNA (*System Network Architecture*), architettura della rete IBM;
- DNA (*Digital Network Architecture*), meglio nota come DECnet, la rete della Digital Eq. Corp.;
- *Internet Protocol Suite*, meglio nota con il nome TCP/IP, è la rete degli elaboratori UNIX e rappresenta uno standard "de facto" attualmente impiegato per la rete Internet di estensione mondiale;
- OSI (*Open System Architecture*), che è lo standard "de iure" in via di completamento nell'ambito dell'ISO.

La figura 2.6 riporta un'analisi comparata tra di esse.

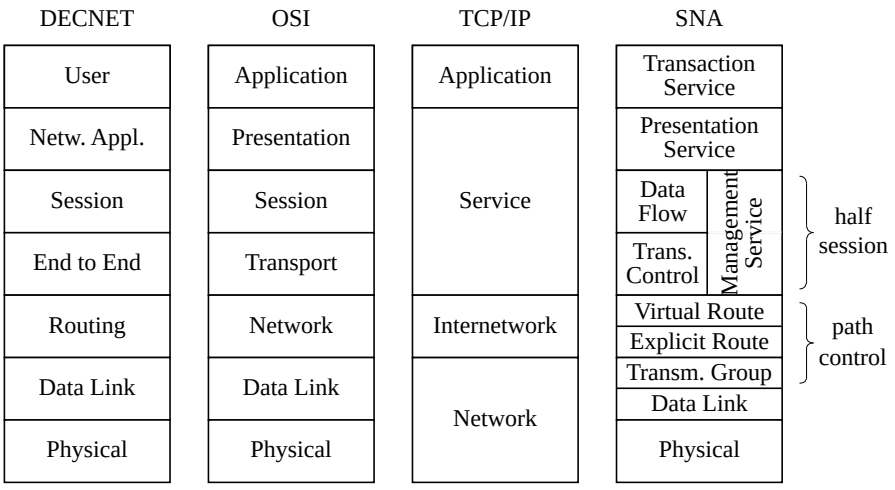


Fig. 2.6 - Principali architetture di rete.

2.6 SISTEMI INTERMEDI

Non sempre lo scambio di informazione avviene direttamente tra i due sistemi finali che contengono le applicazioni *(ES: End Systems)*. Può anche implicare l'attraversamento di sistemi intermedi *(IS: Intermediate Systems)*. In essi esistono delle entità che assumono la funzionalità di *relaying*, cioè di inoltratrici di informazione. Tali entità possono essere collocate a vari livelli del modello OSI e gli IS assumono nomi diversi in funzione del livello a cui avviene il relaying: repeater (livello 1), bridge (livello 2), router (livello 3) e gateway (livello 7). In figura 2.7 è riportato un esempio di utilizzo di router come IS.

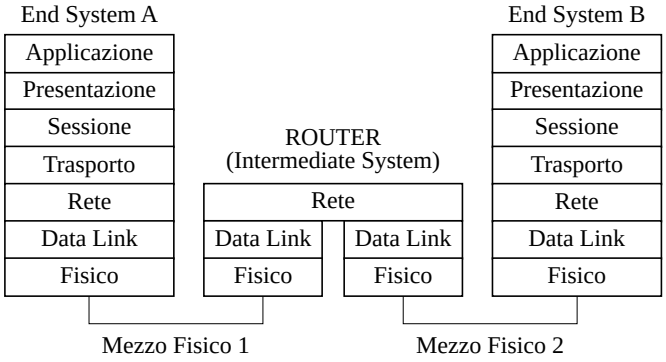


Fig. 2.7 - Esempio di relaying tramite router.

2.7 PROTOCOL DATA UNIT

Ogni livello N aggiunge ai dati ricevuti dal livello superiore alcune informazioni di controllo del protocollo N, dette comunemente "busta di livello N".

Il tutto rappresenta i dati che verranno passati al livello inferiore che opererà in modo analogo. I dati generati da un protocollo di livello N sono detti *N-PDU (Protocol Data Unit)*. Essi diventano, una volta attraversata l'interfaccia tra il livello N e il livello N-1, una *(N-1)-SDU* (*Service Data Unit*), come evidenziato in figura 2.8. La PDU di livello N-1 viene quindi costruita preponendo alla (N-1)-SDU una *(N-1)-PCI (Protocol Control Information)*. Scopo della PCI è quello di contenere le informazioni di controllo del protocollo.

Molto spesso al termine PDU vengono sostituiti quelli meno precisi, ma di uso comune, di pacchetto o trama. Nell'ambito di un pacchetto il PCI rappresenta l'header del pacchetto stesso, già definito busta.

In figura 2.8 è stata fatta l'ipotesi semplificativa che il protocollo non frammenti i dati prima di trasmetterli.

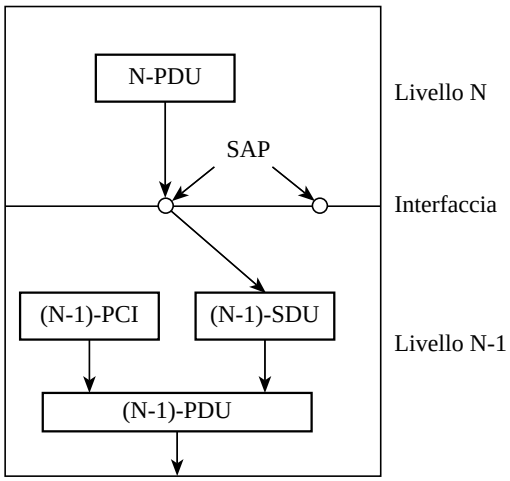


Fig. 2.8 - Relazione tra livelli.

La trasmissione dei dati avviene quindi attraverso una serie di passaggi da livelli superiori a livelli inferiori in un primo sistema, quindi attraverso mezzi fisici di comunicazione, e poi attraverso un'altra serie di passaggi, questa volta da livelli inferiori a livelli superiori, in un secondo sistema (figura 2.9).

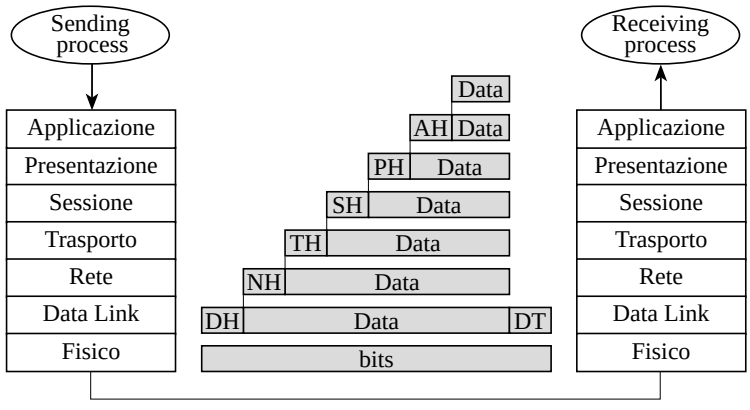


Fig. 2.9 - Imbustamento multiplo.

Si noti che viene aggiunto un header e in un caso un trailer per ogni livello attraversato.

2.8 IL LIVELLO 7: APPLICAZIONE

Il livello 7 è il livello *Applicazione*, cioè dei programmi applicativi (facenti parte del sistema operativo o scritti dagli utenti) attraverso i quali l'utente finale utilizza la rete; esempi di tali applicativi sono: VT (*Terminale Virtuale*), cioè connessione interattiva ad un elaboratore remoto, FTAM (*File Transfer and Access Management*), X.400 (la posta elettronica) e X.500 (*Directory Service*).

2.9 IL LIVELLO 6: PRESENTAZIONE

Il livello 6 è il livello *Presentazione*, che gestisce la sintassi dell'informazione da trasferire (ad esempio codifica ASCII o EBCDIC); a questo livello sono previste tre diverse sintassi: astratta (definizione formale dei dati che gli applicativi si scambiano, come in ISO 8824 o in ASN.1), concreta locale (come i dati sono rappresentati localmente) e di trasferimento (come i dati sono codificati durante il trasferimento).

2.10 IL LIVELLO 5: SESSIONE

Il livello 5 è il livello *Sessione*, responsabile dell'organizzazione del dialogo tra due programmi applicativi e del conseguente scambio di dati; esso consente di aggiungere a connessioni end-to-end (cioè tra due entità collocate in ES) servizi più avanzati, quali la gestione del dialogo (mono o bidirezionale), la gestione del token (per effettuare mutua esclusione nell'utilizzo di una risorsa condivisa) o la sincronizzazione (inserendo dei checkpoint in modo da ridurre la quantità di dati da ritrasmettere in caso di gravi malfunzionamenti).

2.11 IL LIVELLO 4: TRASPORTO

Il livello 4 è il livello *Trasporto*, e fornisce trasferimento trasparente di informazione tra entità del livello sessione. In particolare, si occupa di fornire un trasferimento dati affidabile e di ottimizzare l'uso delle risorse di rete. Compiti del livello 4 saranno quindi tipicamente la frammentazione, la correzione degli errori e la prevenzione della congestione della rete. Il livello 4 è il più basso livello a trascurare la topologia della rete e la presenza di sistemi intermedi (IS) e quindi è il primo livello detto *end-to-end*.

2.12 IL LIVELLO 3: NETWORK

Il livello 3 è il livello *Network*, che gestisce l'instradamento dei messaggi; esso determina se e quali sistemi intermedi devono essere attraversati dal messaggio per giungere a destinazione, quindi deve gestire delle tabelle di instradamento e provvedere ad instradamenti alternativi in caso di guasti (fault tolerance).

2.13 IL LIVELLO 2: DATA LINK

Il livello 2 è il livello *Data Link*, che ha come scopo la trasmissione sufficientemente affidabile di trame (*frame*); accetta come input dei pacchetti di livello 3 (tipicamente poche centinaia di bit) e li trasmette sequenzialmente. Esso verifica la presenza di errori aggiungendo delle FCS (*Frame Control Sequence*) e può gestire meccanismi di correzione di tali errori tramite ritrasmissione.

2.14 IL LIVELLO 1: FISICO

Il livello 1 del modello OSI è il livello *Fisico*, che si occupa di trasmettere sequenze binarie sul canale di comunicazione; a questo livello si specificano, ad esempio, le tensioni che rappresentano 0 e 1 e le caratteristiche dei cavi e dei connettori.

2.15 NOMI E INDIRIZZI

Il modello di riferimento OSI discrimina tra il *nome (title)* di una entità e la sua collocazione all'interno di un sistema, cioè il suo *indirizzo (address)* dato dalla concatenazione di SAP necessari per raggiungere attraverso i vari livelli tale entità. Questo ha il vantaggio di consentire l'accesso ad una entità anche se questa viene spostata da un sistema ad un altro. Tale distinzione impone l'esistenza di un *directory* (spesso detto anche name-server) per tradurre nomi in indirizzi e viceversa.

In particolare l'indirizzo di un applicativo sarà dato come la seguente concatenazione di una serie di SAP:

Indirizzo Applicativo = PSAP + SSAP + TSAP + NSAP

dove PSAP è il Presentation SAP, ecc. Un sistema è identificato in rete da un nome cui corrisponde un NSAP. L'indirizzo di livello 2 (Data Link) è ricavabile tramite opportuni algoritmi a partire da NSAP e viceversa. Molto spesso, in pratica, PSAP e SSAP coincidono e spesso si usa la notazione P/SSAP.

Infine occorre osservare che, nel caso che un applicativo abbia più di una connessione attiva contemporaneamente ad altri applicativi (caso tipico dei server), non è compito del suo indirizzo distinguere tra le varie connessioni, ma tale ruolo viene svolto da un *identificatore di connessione (connection endpoint identifier o instance number)*. Per esempio un server FTAM può avere più connessioni attive tutte identificate dallo stesso indirizzo, ma con identificatori di connessione diversi.

2.16 LE PRIMITIVE OSI

Il modello di riferimento OSI standardizza la modalità di utilizzo dei servizi offerti da un dato livello N ad un livello N+1. Lo standard prevede quattro primitive di servizio: *Request*, *Indication*, *Response* (non è usata a livello 2) e *Confirm*; il diagramma temporale della figura 2.10 ne illustra l'uso.

Le modalità operative previste sono due:

- servizi con conferma (*confirmed*): in tali servizi il livello N+1 ricevente conferma l'avvenuta ricezione;
- servizi senza conferma (*unconfirmed*): in tali servizi il livello N+1 ricevente non conferma l'avvenuta ricezione.

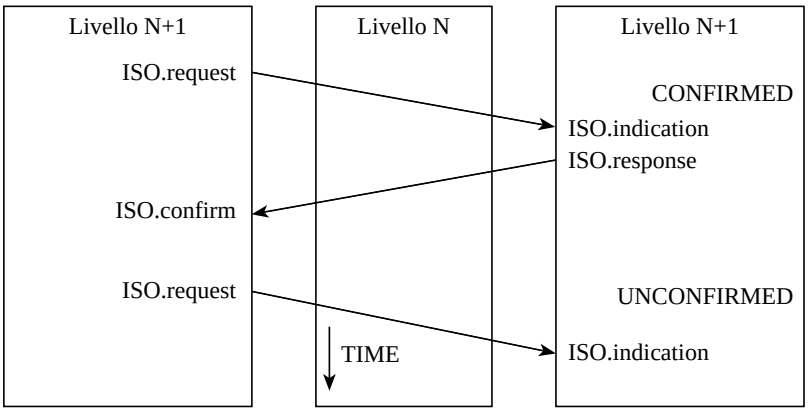


Fig. 2.10 - Primitive OSI.

2.17 PROTOCOLLI CONNESSI E NON

Per tutti i livelli superiori al livello fisico sono definite due modalità operative: una modalità *connessa (CONS: Connection Oriented Network Service)* e una modalità non connessa *(CLNS: ConnectionLess Network Service).* Un dato livello può fornire al livello superiore servizi di tipo connesso, non-connesso o entrambi. Questa è una scelta progettuale che varia per ogni livello, da architettura ad architettura. Lo standard originale ISO 7498 prevedeva solo la modalità connessa ma, vista l'importanza della modalità non connessa, è stata aggiunta in seguito come emendamento allo standard stesso (ISO 7498/Addendum 1).

In un servizio non connesso la spedizione di un pacchetto è simile alla spedizione di una lettera ordinaria con il sistema postale. Tutto avviene in una sola fase lasciando cadere la lettera nella buca delle lettere. La lettera deve contenere sulla busta l'indirizzo completo del destinatario. Non vi è alcun riscontro diretto che la lettera giunga a destinazione correttamente.

In un servizio connesso lo scambio di dati tramite pacchetti ricorda le frasi scambiate tra due interlocutori al telefono. Vi sono tre momenti principali:

- creazione della connessione (il comporre il numero telefonico e il "pronto" alla risposta);
- trasferimento dei dati (la conversazione telefonica);
- chiusura della connessione (i saluti finali e il posare il microtelefono).

2.17.1 La modalità connessa

Nella modalità connessa lo scambio di dati avviene tramite le tre fasi viste prima. Durante la fase di creazione della connessione (*initial setup*) due peer-entities concordano che trasferiranno delle PDU. Solo durante tale fase devono essere specificati gli indirizzi completi del mittente e del destinatario: successivamente le entità coinvolte specificheranno soltanto l'identificativo della connessione stabilito durante la prima fase. Un servizio connesso fornisce una modalità di trasferimento delle PDU affidabile e sequenziale. Per tutta la durata della connessione le PDU inviate sono ricevute correttamente nello stesso ordine. Se qualcosa non funziona correttamente, la connessione può essere riavviata (*reset*) o terminata (*released*). Per verificare che tutte le PDU inviate giungano a destinazione correttamente un servizio connesso utilizza degli schemi di numerazione dei pacchetti e di verifica dell'avvenuta corretta ricezione (ACK: acknowledgement). Quindi un protocollo connesso è in generale in grado non solo di rilevare la presenza di errori, ma anche di correggerli tramite ritrasmissioni.

2.17.2 La modalità non connessa

Con una modalità non connessa la comunicazione ha luogo in una fase singola: il pacchetto è inviato e deve contenere l'indirizzo completo del destinatario. Non essendo i pacchetti organizzati in una connessione, un pacchetto non può fare riferimento ad altri pacchetti trasmessi precedentemente o in seguito. Quindi un protocollo non connesso può solo rilevare la presenza di errori (scartando quindi le PDU errate), ma non correggerli in quanto non si possono realizzare meccanismi di ritrasmissione (in un pacchetto non è possibile fare riferimento ad altri pacchetti).

Un protocollo non connesso è in generale più efficiente di un protocollo connesso, specialmente se bisogna trasferire piccole quantità di dati: in quest'ultimo caso infatti l'overhead della creazione e distruzione della connessione è rilevante.

Un protocollo non connesso (detto anche *datagram*), non potendo garantire l'affidabilità del trasferimento dati, necessita che almeno un protocollo di livello superiore sia di tipo connesso.

Un'analisi comparata tra i due tipi di protocollo è fornita in tabella 2.1.

Caratteristica	Connection-Oriented	Connectionless
Initial setup	Richiesto	Impossibile
Indirizzo di destinazione	Durante il setup	In ogni pacchetto
Ordine dei pacchetti	Garantito	Non garantito
Controllo degli errori	Si	No
Controllo di flusso	Si	No
Negoziazione di opzioni	Si	No
Identificatore di connessione	Si	No

Tab. 2.1 - Analisi comparata.

2.17.3 Applicazioni connesse e non

Anche le applicazioni possono operare in modo connesso oppure no. Un'applicazione infatti può non essere interessata a sapere se i propri dati sono giunti a destinazione o può implementare suoi schemi proprietari di controllo end-to-end. Si pensi ad esempio ad una applicazione che fornisca l'ora esatta a tutti i calcolatori della rete: essa può addirittura ignorare quali siano i calcolatori a cui fornisce il servizio e quindi operare in modo connectionless. Le applicazioni connesse sono molte, ad

esempio quelle di trasferimento file e di posta elettronica.

Chiaramente sia applicazioni connesse che non connesse devono poter operare su di una rete che ai livelli inferiori ha protocolli di tipo connesso oppure no.

Le possibili combinazioni tra livelli connessi e non nel modello OSI sono riportate in figura 2.11.

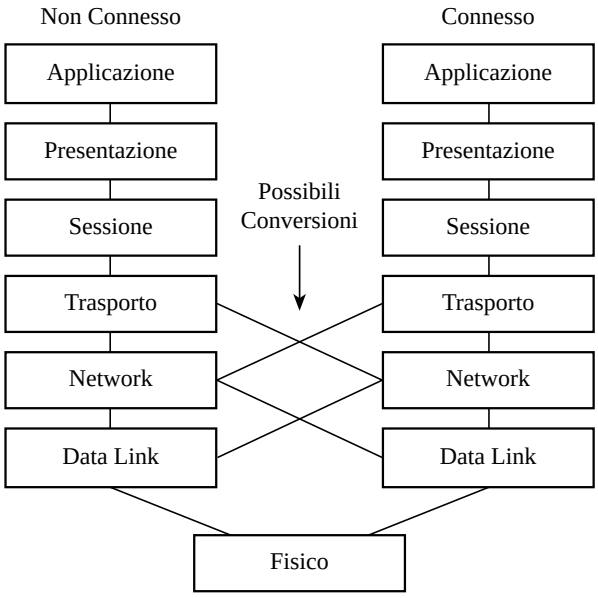


Fig. 2.11 - Possibili conversioni tra modalità connessa e non.

Il livello 1 non può essere considerato né connesso né non connesso; i livelli 2, 3 e 4 possono operare in entrambe le modalità e in tutte le possibili combinazioni. I livelli 5, 6 e 7 devono comportarsi globalmente in modo connesso o non connesso.

A livello 2 l'operatività è normalmente di tipo non connesso quando si opera su reti locali, dove il mezzo trasmissivo è intrinsecamente affidabile, mentre è di tipo connesso su reti geografiche che sono intrinsecamente caratterizzate da un più alto tasso di errore.

A livello 3, vi è sempre stata controversia tra gli informatici che vogliono un livello 3 non connesso e i telecomunicazionisti che lo vogliono connesso. Occorre anche evidenziare come negli ultimi anni il livello 3 sia sempre più stato considerato di competenza degli informatici e quindi si utilizzino sempre più protocolli non connessi.

Il livello 4 è in pratica sempre connesso: infatti, anche quando opera su un livello 3 connesso, l'affidabilità che tale livello 3 fornisce non è ritenuta soddisfacente.

2.18 RELAZIONE TRA OSI E ALTRI STANDARD

L'ISO, dopo aver definito il modello di rifermento OSI, si è posta l'obiettivo di sviluppare altri standard da collocare ai vari livelli. Parte di questi standard sono stati sviluppati direttamente dall'ISO stessa, altri sono stati demandati ad organizzazioni prestigiose quali IEEE, ANSI, CCITT, ecc.

In particolare, agli standard di livello 1 e 2 per le reti geografiche (WAN) ha collaborato il CCITT, mentre per la standardizzazione delle rete locali e metropolitane (LAN/MAN) è stato creato dall'IEEE un apposito progetto, detto progetto IEEE 802 e descritto nel capitolo 5. La relazione tra detti progetti è illustrata in figura 2.12.

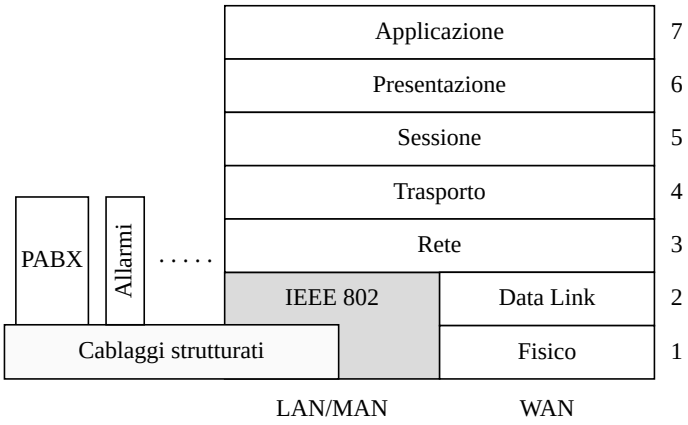


Fig. 2.12 - Relazioni tra standard.

Il progetto IEEE 802 per il livello fisico proponeva mezzi trasmissivi "proprietari", non compatibili con quelli di altri cablaggi per il trasferimento di altri tipi di informazione (es.: allarmi, video, telefonia). Negli ultimi anni c'è stata una forte spinta ad unificare tali cablaggi e sono nati gli standard EIA/TIA 568 e ISO/IEC 11801 che hanno lo scopo di proporre un cablaggio standard unificato che possa essere la base su cui trasmettere sia dati tramite LAN, sia voce tramite PABX (centralini telefonici privati), sia altri tipi di informazione necessari a realizzare un "edificio intelligente". Nel capitolo 3 verranno illustrati i mezzi trasmissivi oggi utilizzati, mentre nel capitolo 4 verranno affrontate le problematiche del cablaggio strutturato degli edifici.

2.19 I PRINCIPALI PROTOCOLLI OSI

La figura 2.13 riporta le sigle dei principali protocolli adottati ai vari livelli del modello di riferimento ISO/OSI.

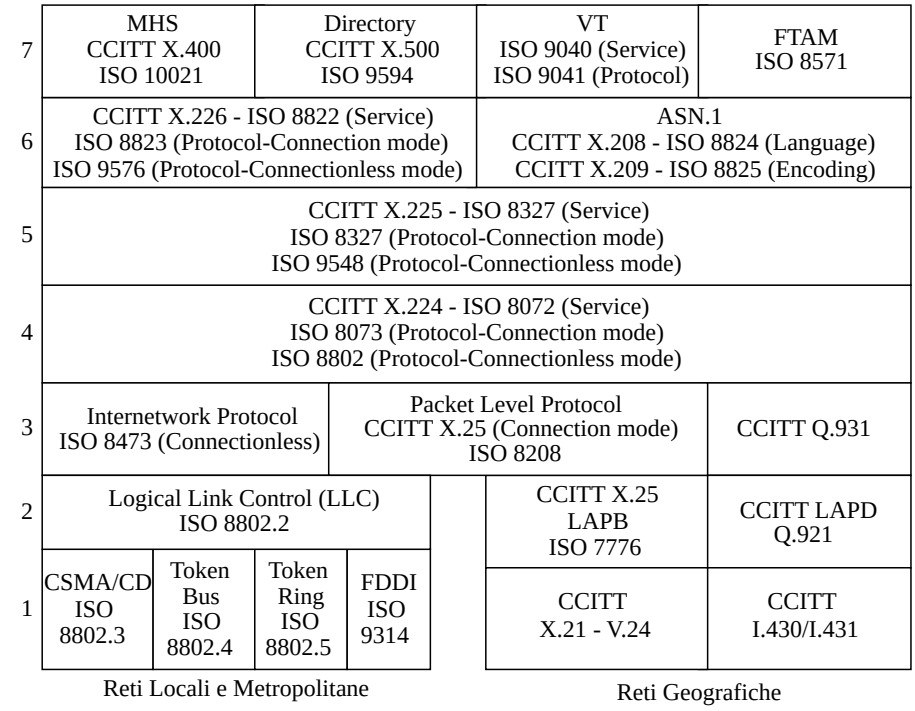


Fig. 2.13 - Principali protocolli OSI.

BIBLIOGRAFIA

[1] ISO 7498, "Data Processing, Open System Interconnection, Basic Reference Model".

[2] Fred Halsal, "Data Communications, Computer Networks and OSI", Addison-Wesley, 1988.

[3] H. Zimmerman, "OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnections,"IEEE Trans. on Communications, Vol. COM-28, No. 4, April 1980, pp. 425-432.

3

I MEZZI TRASMISSIVI

Per realizzare le tipologie di rete precedendemente elencate (LAN, MAN e WAN) è necessario collegare fisicamente gli elaboratori e le apprecchiature di rete mediante opportuni mezzi trasmissivi. La varietà di mezzi trasmissivi oggi disponibili è notevole, e la scelta determina diverse possibili tipologie di impiego (punto-punto, punto-multipunto o broadcast) nonché un'ampia gamma di velocità di trasmissione: da poche centinaia di bit al secondo (b/s) a miliardi di bit al secondo (Gb/s). Il presente capitolo tratterà soltanto i mezzi più utilizzati nella realizzazione di LAN. La tipologia di impiego determina a sua volta quali topologie sono realizzabili. Queste sono di importanza fondamentale per quanto riguarda le tecniche di instradamento dei messaggi, la tolleranza ai guasti e, più in generale, l'organizzazione logica dei protocolli di livello superiore.

3.1 LA TRASMISSIONE DELLE INFORMAZIONI

Come è noto, la trasmissione delle informazioni in forma digitale, cioè la cosiddetta trasmissione dati, richiede innanzitutto la codifica di tali informazioni in termini di bit. Esempi di codifiche sono la tabella ASCII per i caratteri alfanumerici e il PCM (Pulse Code Modulation) per i segnali analogici, che possono rappresentare voce, musica, ecc. I dati digitali così ottenuti vengono poi trasmessi associando ogni bit ad un fenomeno fisico che può essere riprodotto a distanza attraverso il mezzo trasmissivo utilizzato. Si effettua a tal fine un'ulteriore codifica, che in alcuni casi può essere piuttosto complessa, come si vedrà più avanti.

I mezzi trasmissivi utilizzati nelle reti di calcolatori si suddividono attualmente in tre categorie, in base al tipo di fenomeno fisico utilizzato per la trasmissione dei bit:

- mezzi elettrici: sono i mezzi trasmissivi classici del passato, che sfruttano la proprietà dei metalli di condurre l'energia elettrica. Per trasmettere i dati si associano ai bit particolari *valori* di tensione o di corrente, o determinate *variazioni* di tali grandezze.
- onde radio (detti mezzi "wireless"): sono stati introdotti successivamente ai mezzi elettrici, e le applicazioni spaziano dalle reti locali (anche se di diffusione abbastanza ridotta) ai collegamenti via ponte radio o satellite per reti geografiche. In essi, il fenomeno fisico utilizzato è l'onda elettromagnetica, una combinazione di un campo elettrico ed un campo magnetico variabili, che ha la proprietà di propagarsi nello spazio e di riprodurre a distanza una corrente elettrica in un dispositivo ricevente (antenna).
- mezzi ottici: laser e fibre ottiche, in cui il fenomeno fisico utilizzato è la luce. Si tratta dei mezzi trasmissivi più recenti, che hanno rivoluzionato il settore delle telecomunicazioni.

3.1.1 Attenuazione, distorsione, rumore, diafonia

Tutti i fenomeni fisici utilizzati si basano sul trasporto di una qualche forma di energia che codifica l'informazione (che chiameremo *segnale*), a cui il sistema fisico attraversato si oppone, determinando una *attenuazione* dell'energia trasmessa. Tale attenuazione è inoltre diversa a seconda della frequenza, e questo determina la necessità di considerare, per ogni mezzo trasmissivo, la sua *banda passante*, cioè l'insieme delle frequenze che possono essere trasmesse senza attenuazione eccessiva. A seconda delle applicazioni, la banda passante può essere definita semplicemente come valori di frequenza minimo e massimo ai quali l'attenuazione raggiunge valori standard (ad esempio si dimezza la potenza del segnale), oppure tramite tabelle che forniscono i valori di attenuazione a diverse frequenze (è questo il caso dei mezzi elettrici adottati nelle LAN). Il diverso comportamento del mezzo trasmissivo in funzione della frequenza genera anche *distorsione*, cioè l'alterazione dell'andamento nel tempo del segnale (tale andamento nel tempo, rappresentabile graficamente, prende il nome di *forma d'onda*). Ad alterare il segnale concorre anche il *rumore*, cioè la sovrapposizione al segnale di energia proveniente da elementi esterni al sistema trasmissivo (ad esempio disturbi elettromagnetici dovuti a linee di alimentazione elettrica) o interni (ad esempio il rumore generato dai dispositivi elettronici

di amplificazione). Poiché le caratteristiche del rumore possono essere note soltanto in termini statistici e non esatti, in fase di ricezione non è in generale possibile distinguere tra segnale originale e rumore, ed è necessario adottare tecniche adeguate per prevenire errori di ricezione a causa del rumore. Un tipo particolare di rumore, frequente nei sistemi trasmissivi adottati per le LAN, è rappresentato dalla *diafonia*. L'energia che si somma a quella del segnale sul mezzo trasmissivo in esame proviene dalla trasmissione di un altro segnale su un altro mezzo trasmissivo analogo in prossimità del primo.

Per tutti i fenomeni appena descritti non è importante quantificarne l'effetto in termini assoluti, bensì in termini relativi, cioè determinare quanto viene alterato il segnale trasmesso. Per questo si usa come unità di misura il *decibel* (dB), grandezza che esprime il rapporto, in termini logaritmici, di due grandezze fisiche. Alcuni esempi:

- *attenuazione* di un segnale elettrico: rapporto tra la tensione del segnale in ingresso al mezzo trasmissivo e la sua tensione in uscita
  $$\text{attenuazione}_{\text{dB}} = 20 \log \frac{V_{in}}{V_{out}}$$
- *rapporto segnale/rumore* (detto anche signal/noise, S/N) in un amplificatore di segnale elettrico: rapporto tra il massimo valore di tensione del segnale ottenibile senza distorsione e il valore della tensione del rumore generato dall'amplificatore stesso
  $$S / N_{\text{dB}} = 20 \log \frac{V_S}{V_N}$$

3.1.2 Mb/s e MHz: tecniche di codifica per la trasmissione digitale

Per trasmettere le informazioni codificate in forma digitale è necessario associare ai bit determinati valori del fenomeno fisico scelto. La tecnica più ovvia consiste nell'associare semplicemente due differenti valori per lo zero e per l'uno, ma è possibile adottare tecniche più sofisticate, che garantiscono una corretta sincronizzazione del ricevitore con il trasmettitore e che permettono di ridurre la banda necessaria alla trasmissione e quindi la banda passante richiesta al mezzo trasmissivo. Una caratteristica importante delle tecniche di codifica, infatti, è il numero di variazioni del segnale necessarie per codificare un bit. Questo determina, a partire dalla velocità di trasmissione dei bit, misurata in bit al secondo (bps o b/s), la frequenza con cui varia il segnale, misurata in hertz (Hz, "pulsazioni al secondo"), che deve cadere all'interno della banda passante del mezzo trasmissivo.

È importante notare che tale frequenza rappresenta solamente il valore minimo di banda passante che il mezzo deve offrire, in quanto qualsiasi segnale non sinusoidale (come l'onda quadra generata nella trasmissione di segnali digitali), è composto, oltre che dalla fondamentale, anche da un numero teoricamente infinito di *armoniche*, segnali sinusoidali a frequenza multipla della fondamentale. La distorsione del segnale è tanto minore quante più armoniche sono trasmesse con attenuazione trascurabile.

Nei mezzi trasmissivi utilizzati nelle LAN, comunque, l'attenuazione aumenta con la frequenza in modo abbastanza graduale, e, per ogni standard di codifica, la massima attenuazione consentita è in genere specificata fino a frequenze di poco superiori a quella della fondamentale.

Le codifiche utilizzate nell'ambito delle LAN sono: *NRZ*, *Manchester*, *NRZI*, *MLT-3*. Nelle descrizioni che seguono, verranno indicati con "alto"e "basso"("high"e "low") due possibili stati del fenomeno fisico usato per la trasmissione.

Codifica NRZ

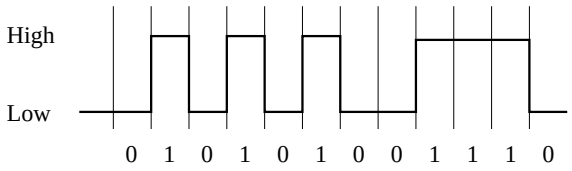


Fig. 3.1 - Codifica NRZ.

La codifica più semplice consiste nell'associare a ciascun bit un valore stabile per la sua intera durata. Tale codifica prende il nome di NRZ (*Non Return to Zero*, figura 3.1), ed è equivalente alla rappresentazione in termini di zeri e uni.

Ai fini della trasmissione, si determinano le principali caratteristiche di una codifica in base ai due casi estremi di massimo e minimo numero di transizioni generate nell'unità di tempo.

Il minimo numero di transizioni nell'unità di tempo determina la possibilità di sincronizzazione del ricevitore. Nel caso della codifica NRZ una sequenza di valori uguali non genera alcuna transizione, e, pertanto, risulta impossibile garantire la corretta sincronizzazione. Questo problema viene aggirato ricodificando e allungando le sequenze di bit da trasmettere in modo da garantire sempre, in funzione della codifica sul mezzo fisico, un certo numero minimo di transizioni. Esempi di tali codifiche sono *4B5B*, *5B6B*, discusse nel paragrafo 3.1.3.

Il massimo numero di transizioni nell'unità di tempo permette di determinare la frequenza *fondamentale* del segnale trasmesso nel caso peggiore (massima richiesta di banda). Trattandosi di un segnale ad onda quadra, la fondamentale è rappresentata dal segnale sinusoidale che la approssima, e a cui è associato il maggior contenuto in termini di potenza.

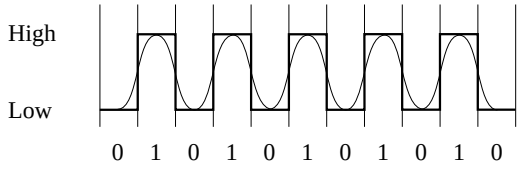


Fig. 3.2 - Frequenza fondamentale nella codifica NRZ.

Come risulta evidente dalla figura 3.2, nella codifica NRZ ogni bit occupa un semiciclo della fondamentale, e pertanto questa ha frequenza pari alla metà della frequenza di bit. Per esempio, una trasmissione a 1 Mb/s presenterà una frequenza fondamentale massima di 500 KHz.

L'utilizzo della codifica NRZ con 5B6B è previsto dallo standard 802.12 per la trasmissione a 100 Mb/s su cavo in rame a due o a quattro coppie e su fibra.

Codifica Manchester

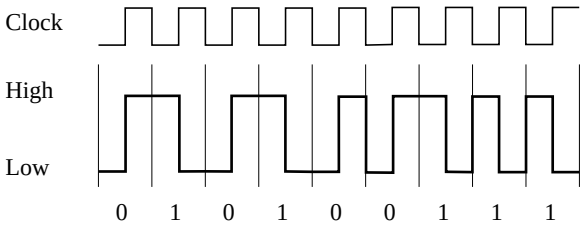


Fig. 3.3 - Codifica Manchester.

Nella codifica Manchester (figura 3.3), il segnale di clock del trasmettitore (1 ciclo = 1 bit) e il segnale di dato vengono combinati per garantire la presenza di almeno una transizione per ogni bit. In pratica, ogni bit è codificato trasmettendo un ciclo del segnale di clock, inalterato quando si trasmette uno zero, invertito quando si trasmette un uno.

Il massimo numero di transizioni viene generato trasmettendo sequenze di valori uguali. In tal caso il segnale inviato è in pratica il clock del trasmettitore, e la fondamentale ha frequenza pari alla frequenza di bit. Per una trasmissione a 10 Mb/s, quindi, la frequenza è di 10 MHz. Al vantaggio di una facile sincronizzazione si contrappone quindi lo svantaggio di una banda richiesta doppia rispetto alla codifica NRZ.

La codifica Manchester è utilizzata nelle reti Ethernet (802.3) a 10 Mb/s e Token Ring (802.5).

Codifica NRZI

La codifica NRZI (*Non Return to Zero Inverted on one*, figura 3.4), prevede una transizione per i bit a uno, a metà del bit, e nessuna transizione per i bit a zero. La transizione per i bit a uno può essere "alto-basso" o "basso-alto", a seconda dello stato del segnale in corrispondenza del bit precedente. Pertanto, si ottiene il massimo numero di transizioni con una sequenza di uni, e anche in questo caso, come già per NRZ, ogni bit occupa un semiciclo della fondamentale (figura 3.5), e quindi la frequenza della fondamentale risulta essere pari alla metà della frequenza di bit. Per esempio, la codifica NRZI è utilizzata per FDDI su fibra ottica, che a livello fisico opera a 125 Mb/s e quindi la frequenza della fondamentale è 62.5 MHz.

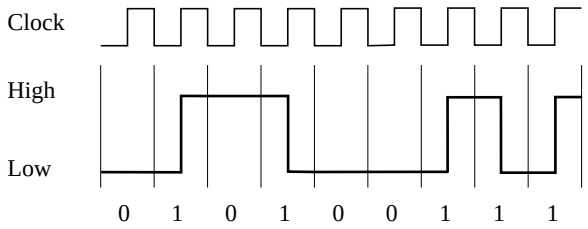


Fig. 3.4 - Codifica NRZI.

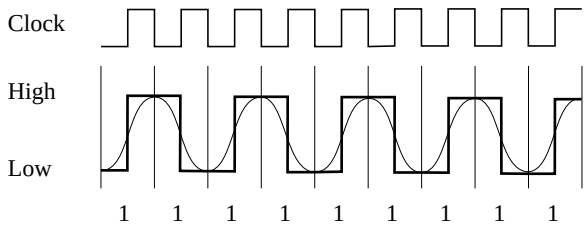


Fig. 3.5 - Frequenza fondamentale nella codifica NRZI.

Per quanto riguarda la sincronizzazione, l'unico vantaggio che la codifica NRZI offre rispetto alla codifica NRZ consiste nel fatto che per garantire la presenza di una transizione è sufficiente garantire la presenza di un uno, e non, come per NRZ, di una sequenza uno-zero o zero-uno. Resta il problema di sincronizzare il ricevitore quando si trasmette una lunga sequenza di zeri. Anche in questo caso si ricorre ad un'ulteriore codifica, 4B5B nel caso di FDDI su fibra ottica.

Codifica MLT-3

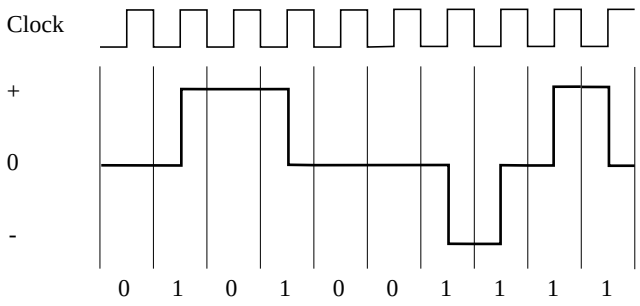


Fig. 3.6 - Codifica MLT-3.

A differenza delle codifiche viste finora, la codifica MLT-3 (figura 3.6) opera su tre livelli anziché su due. Nel caso di trasmissione su mezzo elettrico, per esempio, i tre livelli potranno essere rappresentati da una tensione positiva, una tensione negativa, e assenza di tensione (0 volt). Per quanto riguarda la codifica dei bit, invece, funziona in modo simile alla NRZI, in quanto prevede una transizione a metà dei bit a 1 e nessuna transizione per i bit a zero. Le transizioni per i bit a uno si susseguono nell'ordine: $0 \rightarrow +$, $+ \rightarrow 0$, $0 \rightarrow -$, $- \rightarrow 0$, ecc.

Anche per la codifica MLT-3 il massimo numero di transizioni è dato da una sequenza di valori a uno. Tuttavia, la particolare codifica su tre valori fa sì che la frequenza della fondamentale sia soltanto un quarto della frequenza di bit (figura 3.7).

La codifica MLT-3 è utilizzata da FDDI TP-PMD e da Ethernet IEEE 802.3 100BaseTX, due standard per trasmissioni a 100 Mb/s su cavi in rame. Per FDDI e Ethernet la velocità di trasmissione sul mezzo trasmissivo è di 125 Mb/s, e quindi la frequenza della fondamentale è di 31.25 MHz. La differenza di 25 Mb/s tra la velocità nominale al livello Data Link (100 Mb/s) e la velocità a livello Fisico (125 Mb/s) è dovuta al fatto che l'assenza di transizioni per sequenze di bit a zero

impone, anche in questo caso, una ricodifica 4B5B delle sequenze da trasmettere. MLT-3 è anche stata proposta dall'ATM Forum per la trasmissione a 155 Mb/s su rame, con codifica 4B5B, per cui la frequenza della fondamentale risulta essere di 48.4375 MHz.

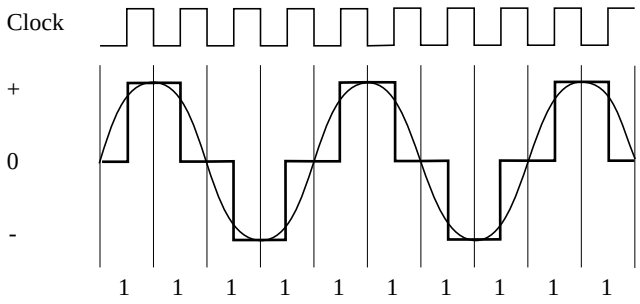


Fig. 3.7 - Frequenza fondamentale nella codifica MLT-3.

La codifica MLT-3 necessita di un rapporto segnale/rumore sul canale trasmissivo maggiore di 3-4 dB rispetto alla codifica NRZ, in quanto quest'ultima utilizza soltanto due livelli. In compenso presenta una minore emissione di radiodisturbi: una codifica MLT-3 a 125 Mb/s presenta limitate emissioni elettromagnetiche a frequenze appena poco superiori a 30 MHz.

Tecniche avanzate di codifica

A causa dell'utilizzo diffuso di doppini privi di schermatura, o schermati ma soltanto globalmente e non coppia per coppia, è sempre più sentito il problema della compatibilità elettromagnetica, problema che si accentua al crescere della velocità trasmissiva.

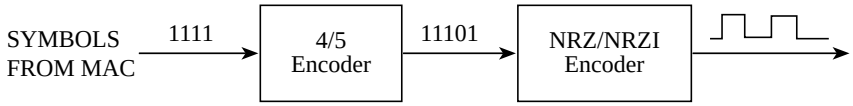
Una soluzione interessante consiste nell'adottare tecniche di codifica sofisticate che derivano dallo studio matematico del comportamento di particolari segnali sia nel dominio del tempo che della frequenza. Una classe di codifiche di questo tipo prende il nome di codifiche a risposta parziale (*partial response*), in cui in fase di ricezione al simbolo corrente si sovrappongono "code" dei simboli precedentemente trasmessi (interferenza intersimbolica), ma in modo controllato e quindi eliminabile. Esempi di tali codifiche sono le BPR1 e BPR4, a tre livelli, e la QPR4, a sette livelli. Queste codifiche permettono di ridurre le emissioni di radiodisturbi pur richiedendo un limitato aumento del rapporto segnale/rumore (0.5-1 dB) rispetto alla codifica NRZ.

Altre codifiche proposte per consentire elevate velocità trasmissive su doppino non schermato prendono spunto dalle tecniche utilizzate nei modem, basate su modulazioni di fase e di ampiezza e opportuni filtri nel ricevitore.

3.1.3 Codifiche 4B5B, 5B6B, 8B6T

Per tutte le tecniche di codifica viste, ad eccezione della Manchester, esistono sequenze di dati che non generano transizioni. Per garantire la trasmissione di un numero di transizioni sufficiente a consentire la sincronizzazione del ricevitore, è necessario ricodificare i dati da trasmettere, eventualmente allungandone la sequenza. Esistono due standard per fare questo: la codifica 4B5B, che codifica in cinque bit ogni possibile sequenza di quattro bit ed è usata in combinazione con NRZI o MLT-3, e la codifica 5B6B, che trasforma quintetti di bit in sequenze da sei ed è usata nello standard 802.12 unitamente alla codifica NRZ.

Lo schema di impiego della codifica 4B5B per FDDI su fibra ottica è illustrato in figura 3.8.



1111 è il simbolo per il dato F
11101 è il codice di gruppo per il dato F

Fig. 3.8 - Esempio di codifica 4B5B.

La codifica e la relativa decodifica avvengono tramite tabelle. In tabella 3.1 è riportata la codifica dei principali simboli MAC in 4B5B.

Come si può osservare, la codifica 4B5B comprende tutti i possibili quartetti in ingresso, più alcuni simboli aggiuntivi per la gestione di un protocollo a livello fisico. L'overhead introdotto è pari ad un bit ogni quattro, cioè il 25%. Una trasmissione a 100 Mb/s al livello MAC, quindi, invierà sul mezzo fisico 125 Mb/s.

Lo schema di codifica 5B6B trasforma quintetti di bit in gruppi da sei ed è più complesso, in quanto opera in due stati possibili (detti "modo 2" e "modo 4"). I due modi differiscono dal numero di uni presenti in ogni gruppo di sei bit, e vengono ciclicamente alternati per bilanciare il numero totale di zeri e di uni trasmessi.

Valore	Simbolo	Assegnazione
00000	Q	stato di linea Quiet
11111	I	stato di linea Idle
00100	H	stato di linea Halt
11000	J	prima parte dello start delimiter
10001	K	seconda parte dello start delimiter
11110	0	quartetto di valore 0
01001	1	quartetto di valore 1
10100	2	quartetto di valore 2
10101	3	quartetto di valore 3
01010	4	quartetto di valore 4
01011	5	quartetto di valore 5
01110	6	quartetto di valore 6
01111	7	quartetto di valore 7
10010	8	quartetto di valore 8
10011	9	quartetto di valore 9
10110	A	quartetto di valore A
10111	B	quartetto di valore B
11010	C	quartetto di valore C
11011	D	quartetto di valore D
11100	E	quartetto di valore E
11101	F	quartetto di valore F
01101	T	simbolo di terminazione
00111	R	zero logico (reset)
11001	S	uno logico (set)

Tab. 3.1 - Codifica dei simboli in 4B5B.

Infine, la codifica 8B6T è utilizzata in Ethernet 802.3 100BaseT4 per convertire ottetti in gruppi di sei simboli ternari. Si tratta di una codifica unica che evita il doppio passaggio 4B5B e poi MLT-3 di FDDI TP-PMD. Lo schema di codifica 8B6T definisce 256 parole di codice basate su simboli ternari ("+", "-" e "0"), equivalenti ai 256 valori rappresentabili su 8 bit. La tabella di codifica è costruita in modo tale da garantire un numero di transizioni sufficiente alla sincronizzazione.

3.1.4 Scrambling

Gli schemi di codifica appena discussi hanno come obiettivo garantire, nell'unità di tempo, un numero minimo di transizioni del segnale. Questo determina

una maggior facilità di sincronizzazione del ricevitore, ma dal punto di vista delle emissioni di disturbi elettromagnetici (e quindi, più in generale, delle interferenze elettromagnetiche, EMI - *Electro Magnetic Interference*) aggrava la situazione, in quanto, generando ripetizioni regolari di sequenze di transizioni simili fra loro, concentra l'emissione in determinate frequenze. L'utilizzo diffuso di doppino non schermato, che fonda la sua capacità di contenere il valore delle emissioni soltanto sulla regolarità della geometria e sulla simmetria del trasmettitore, ha spinto alla definizione di una tecnica di codifica aggiuntiva, basata non su tabelle bensì su funzioni logiche (cioè che trasformano dati binari in ingresso in dati binari in uscita). Tale codifica prende il nome di *scrambling*, ed una proposta di scrambler è contenuta nello standard TP-PMD per FDDI su doppino.

TP-PMD (*Twisted Pair - Physical Medium Dependent*) permette di sostituire il doppino alla fibra in modo trasparente per l'interfaccia collegata al transceiver. Quindi riceve il segnale che normalmente verrebbe trasformato in impulsi luminosi, che come già detto è ottenuto con una codifica 4B5B e poi NRZI, lo ricodifica in NRZ, vi applica la funzione di scrambling e lo codifica in MLT-3.

Lo scrambling permette di ottenere sequenze poco regolari delle transizioni del segnale anche a fronte di sequenze ripetitive di dati da trasmettere. La funzione di scrambling deve essere sufficientemente semplice da poter essere realizzata in hardware, e lo schema del TP-PMD prevede che la sequenza di bit da trasmettere venga sommata, in modulo a 2, ad una sequenza pseudocasuale di 2047 bit detta chiave. La funzione di *descrambling*, cioè di decodifica delle sequenze ricevute, è un po' più complicata a causa della necessità di sincronizzare la chiave del ricevitore con la chiave del trasmettitore. L'operazione di sincronizzazione viene effettuata durante la ricezione di sequenze note di bit, appartenenti al protocollo di gestione della linea e presenti quando non vengono inviati dati.

Anche lo standard 802.12 prevede l'utilizzo di scrambling su ognuno dei quattro canali in cui viene suddivisa la trasmissione (assegnati poi a quattro coppie in rame oppure multiplexati su una singola coppia o su una fibra ottica).

3.2 MEZZI TRASMISSIVI ELETTRICI

I mezzi trasmissivi elettrici rappresentano ancora oggi il mezzo più diffuso, e nell'ambito delle reti locali assumono fondamentale importanza soprattutto per la realizzazione di infrastrutture per la trasmissione di segnali all'interno degli edifici, argomento che verrà trattato in dettaglio nel capitolo dedicato ai cablaggi strutturati.

Dovendo trasportare il segnale in forma di energia elettrica, è necessario che le caratteristiche elettriche del mezzo siano tali da rendere massima la trasmissione dell'energia da un estremo all'altro e minima la dissipazione in altre forme (ad esempio calore, irradiazione elettromagnetica), e la forma d'onda resti il più possibile inalterata. Purtroppo, le caratteristiche costruttive necessarie per conseguire tale obiettivo sono in contrasto con altre esigenze quali flessibilità, sicurezza, ininfiammabilità, ecc. Ciononostante, con l'attuale tecnologia è possibile realizzare mezzi trasmissivi elettrici di caratteristiche sufficientemente elevate da permettere la trasmissione dei dati a velocità superiori a 100 Mb/s.

3.2.1 La sezione dei conduttori

La sezione dei conduttori può essere espressa come misura del diametro in millimetri (valori tipici 0.4 - 0.7 mm), ma questa soluzione è poco usata. Molto più diffusa è l'unità di misura detta AWG (American Wire Gauge).

L'AWG è una scala a regressione geometrica con 39 valori compresi nell'intervallo da 0 gauge (0.460 pollici di diametro) a 36 gauge (0.005 pollici di diametro); ogni incremento di un gauge corrisponde ad un rapporto tra i diametri di $(0.460/0.005)^{1/39} \cong 92^{1/39} \cong 1.229322$. Nella tabella 3.2, sono riportati i valori di AWG più utilizzati nei cavi per TD. Avere un basso AWG, e quindi diametro elevato, è un parametro di merito, in quanto diminuisce la resistenza e quindi la potenza dissipata sul cavo. I diametri dei cavi comunemente usati per la trasmissione dati sono compresi tra 26 AWG (doppini per sola telefonia) e 22 AWG (cavo di tipo 1 IBM).

AWG	mm (Ø)	mm^2	Kg/Km	Ω/Km
22	0.6438	0.3255	2.894	52.96
23	0.5733	0.2582	1.820	84.21
24	0.5106	0.2047	1.746	87.82
25	0.4547	0.1624	1.414	108.4
26	0.4049	0.1288	1.145	133.9

Tab. 3.2 - Diametri dei cavi in rame comunemente usati nella trasmissione dati.

3.2.2 Materiali isolanti e sicurezza in caso di incendio

I materiali isolanti usati nella costruzione dei cavi possono essere di due tipi: compatti o espansi. La scelta determina notevoli differenze nella costante dielettrica, che per l'isolante di un cavo è tanto migliore quanto più vicina a quella dell'aria. Gli isolanti espansi (che contengono aria) sono migliori di quelli compatti, ma presentano due gravi inconvenienti: sono estremamente infiammabili, in quanto contengono sia il combustibile (plastica) che il comburente (aria), e sono più voluminosi, rendendo maggiori le dimensioni dei cavi. Per queste ragioni ormai per quasi tutti i cavi si usano isolanti compatti, molto più sottili e che presentano, in caso d'incendio, un'emissione di fumi limitata e non tossica. Quest'ultimo aspetto è fondamentale in quanto i cavi per trasmissione dati devono sottostare a normative per la sicurezza in caso di incendio. Esistono principalmente due tipi di cavi che possono essere utilizzati: *non plenum* e *plenum*. I primi sono quelli più usati e, a seconda del materiale costituente la guaina esterna, hanno caratteristiche diverse:

- *flame retardant:* ritardano la propagazione della fiamma;
- *low smoke fume (LSF):* bassa emissione di fumi in caso d'incendio;
- *zero halogen (0H):* assenza di emissione di gas tossici.

I cavi di tipo plenum, invece, hanno la proprietà di resistere ad alte temperature, poiché sia il materiale isolante sia la guaina esterna sono in teflon, non propagano l'incendio e non bruciano, ma nel caso peggiore si carbonizzano emettendo gas tossici. Questi tipi di cavi trovano applicazione per ora solo negli Stati Uniti per installazioni in controsoffittatura, quando questa viene utilizzata come condotta di ritorno dell'aria condizionata.

3.2.3 Tecniche di trasmissione

I circuiti elettronici funzionano generalmente controllando correnti o tensioni rispetto ad un unico conduttore di ritorno (per le correnti) o di riferimento (per le tensioni). Le prime tecniche di trasmissione dei segnali digitali erano basate sul medesimo principio: si portava il riferimento di tensione da trasmettitore a ricevitore tramite un conduttore, e il segnale (o i segnali) su un altro conduttore (o su più d'uno). Questa tecnica di trasmissione è detta *sbilanciata* ("longitudinal mode", in inglese). Poiché il conduttore che trasporta il segnale si comporta da antenna nei confronti dei campi elettromagnetici in cui è immerso (disturbi

provenienti da altri conduttori, da impianti elettrici, da trasmissioni radio e TV, ecc.), e la corrente indotta nel conduttore si somma a quella del segnale, rendendone difficile o impossibile la decodifica, per tale tipo di trasmissione si impiega spesso il cavo coassiale. Il foglio o la calza metallica che avvolge il cavo coassiale svolge la triplice funzione di conduttore per il ritorno della corrente del segnale, riferimento di tensione e gabbia di Faraday, cioè schermatura, per il conduttore interno (figura 3.9).

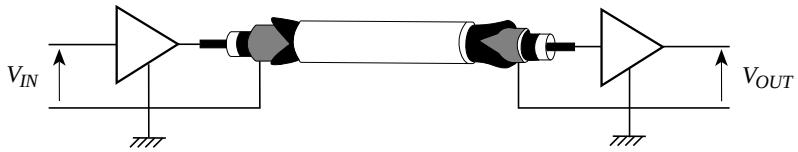


Fig. 3.9 - Trasmissione sbilanciata su cavo coassiale.

Un problema di questo tipo di trasmissione è dovuto al fatto che anche lo schermo si comporta da antenna, e le correnti indotte in esso da parte dei disturbi elettromagnetici, nonché disturbi provenienti dalla messa a terra delle apparecchiature, possono provocare differenze nelle tensioni di riferimento di ricevitore e trasmettitore. Siccome il valore del segnale è misurato relativamente a tali tensioni, ne risulta un'alterazione dei valori ricevuti che può portare ad errori nella trasmissione dei dati.

La tecnica alternativa alla trasmissione sbilanciata è la trasmissione *bilanciata* ("differential mode" in inglese). Essa consiste nell'utilizzare due conduttori perfettamente simmetrici (detti "coppia"), sui quali viene inviato lo stesso segnale elettrico, ma in opposizione di fase (figura 3.10).

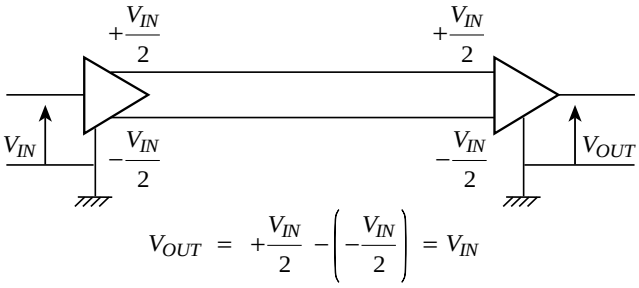


Fig. 3.10 - Trasmissione bilanciata.

Il vantaggio rispetto alla trasmissione sbilanciata consiste nell'assenza della tensione di riferimento che deve essere identica per ricevitore e trasmettitore. Nella trasmissione bilanciata, infatti, il segnale è ricostruito per differenza delle tensioni presenti sui due conduttori della coppia. Presupposto fondamentale per la trasmissione bilanciata è che i due conduttori siano perfettamente simmetrici rispetto a qualsiasi punto dello spazio, in modo da annullare sia l'emissione che la sensibilità ai disturbi elettromagnetici. La perfetta simmetria potrebbe essere raggiunta soltanto se i due conduttori coincidessero, cosa irrealizzabile per il limite minimo nelle dimensioni fisiche e per la necessità di interporre fra essi del materiale isolante, ma può essere approssimata ritorcendo i due conduttori. Si realizza così il "doppino ritorto"(*twisted pair, TP*). La trasmissione bilanciata su TP riduce le emissioni di disturbi elettromagnetici in quanto le correnti che attraversano i due conduttori sono di uguale intensità e verso opposto, e generano campi magnetici opposti che tendono ad annullarsi (figura 3.11).

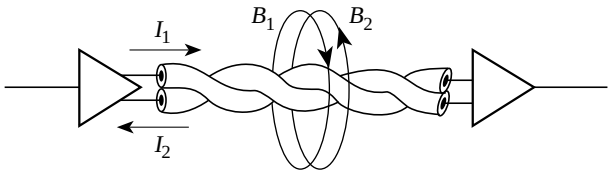


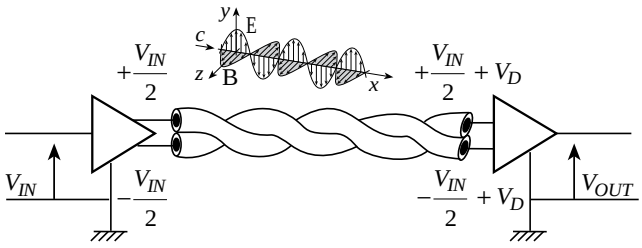
Fig. 3.11 - Trasmissione bilanciata su doppino: riduzione dell'emissione di disturbi.

Mentre la ridotta emissione di disturbi è dovuta alla simmetria nella trasmissione, l'immunità ai disturbi esterni è dovuta all'amplificazione differenziale del segnale nel ricevitore. Grazie alla simmetria del sistema l'onda elettromagnetica illustrata in figura 3.12 induce la medesima tensione di disturbo (V_D) in entrambi i conduttori, e tale termine scompare nella differenza che genera il segnale di uscita.

Soltanto recentemente la tecnologia ha permesso l'applicazione di questo principio a sistemi per trasmissione dati ad alta velocità. Le difficoltà consistono nel produrre doppini a geometria altamente regolare, in cui gli effetti del rumore risultano altamente simmetrici nei due fili, e nel realizzare amplificatori differenziali ad elevata reiezione del modo comune (cioè che misurino la differenza dei segnali con un residuo molto basso di segnale comune), in grado di funzionare a centinaia di MHz.

Da quanto visto è evidente la necessità non soltanto di produrre cavi a geometria estremamente regolare, ma anche e soprattutto garantire che tale geometria sia mantenuta anche dopo la posa del cavo stesso. Questo è invece più

difficile, in quanto le operazioni di posa, specialmente se effettuate per trazione o in canaline strette e tortuose, tendono ad alterare anche notevolmente la geometria del cavo e di conseguenza a peggiorarne le prestazioni. Una geometria regolare non soltanto permette di sfruttare al massimo i vantaggi della trasmissione bilanciata nel caso di doppini, ma rende anche costanti i parametri elettrici del cavo per la sua intera lunghezza, riducendo le variazioni di impedenza e le conseguenti riflessioni di segnale. Proprio per questo i cavi di più recente concezione sfruttano tecniche costruttive sofisticate per garantire geometrie inalterate a cavo posato.



$$V_{OUT} = \left(+\frac{V_{IN}}{2} + V_D\right) - \left(-\frac{V_{IN}}{2} + V_D\right) = V_{IN}$$

Fig. 3.12 - Trasmissione bilanciata su doppino: immunità ai disturbi.

3.2.4 Schermatura

È in continua crescita l'attenzione al problema dei disturbi elettromagnetici (EMI), dei quali le reti locali sono al contempo vittime e sorgenti. Con la presenza di schermi e con una corretta messa a terra si possono ridurre drasticamente la sensibilità e l'emissione di disturbi elettromagnetici, e possono migliorare anche notevolmente le caratteristiche elettriche di un cavo. Esistono numerosi tipi di schermo, tra i quali i più utilizzati nelle LAN sono:

- "foglio" (*foil*): si tratta normalmente di un foglio di alluminio o di mylar alluminato, molto sottile (da 0.05 mm a 0.2 mm) che avvolge il cavo immediatamente sotto alla guaina di protezione esterna. Poiché l'alluminio presenta elevata resistenza elettrica rispetto al rame, e, a spessori così ridotti, una notevole fragilità, lungo il foglio scorre un filo di rame nudo, detto *drain*, che garantisce continuità elettrica anche in caso di eventuali crepe; tale filo è utilizzato per il collegamento di terra;

- "calza" (*braid*): si tratta di una trecciola di fili di rame che avvolgono il cavo in due direzioni opposte. Presenta una conducibilità molto migliore del foglio di alluminio, ma la copertura non è completa, in quanto in corrispondenza degli intrecci rimangono inevitabilmente dei fori nello schermo. Inoltre, l'ossidazione dei fili di rame e la loro deformazione in fase di posa del cavo possono alterare l'efficacia della schermatura.

I migliori risultati si ottengono dalla combinazione di più schermi diversi, come foglio più calza, foglio più calza più foglio, e così via. Tuttavia questo può creare problemi in fase di installazione, soprattutto su certi tipi di connettori non studiati per schermature così complesse, quali gli RJ45 previsti per il cablaggio strutturato degli edifici, di cui si parlerà più avanti.

Nel caso di cavi con più coppie di conduttori, la schermatura può essere applicata all'intero cavo o a tutte le coppie di conduttori singolarmente, riducendo così la diafonia tra le coppie vicine.

L'efficacia della schermatura di un cavo è misurata tramite un parametro detto *impedenza di trasferimento*. Essa è definita come rapporto tra la caduta di tensione che si genera all'interno dello schermo di un cavo e la corrente che vi scorre in superficie indotta dal disturbo elettromagnetico (figura 3.13). L'impedenza di trasferimento, normalmente indicata con Z_t, si misura in mΩ/m, ed è tanto più bassa quanto più lo schermo è efficace.

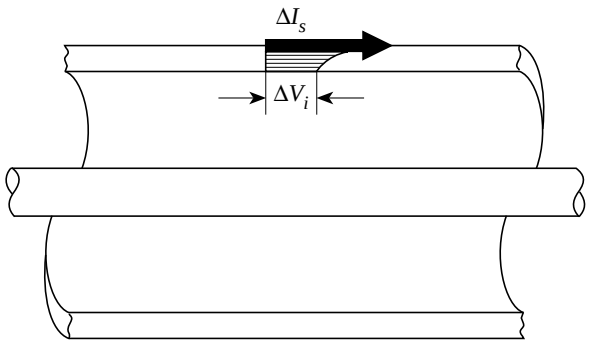


Fig. 3.13 - Impedenza di trasferimento

Va infine ricordato che la presenza di uno schermo può migliorare l'attenuazione dei disturbi esterni e la diafonia, ma soltanto se l'installazione è fatta in modo adeguato. È molto facile ottenere un peggioramento delle prestazioni rispetto a un cavo non schermato, a causa della difficoltà di soddisfare contemporaneamente le

esigenze di messa a terra per la sicurezza elettrica, schermatura contro i disturbi, collegamento delle masse, tensione a 0*V* di riferimento comune alle varie apparecchiature ed evitare i loop di massa. La tecnica di trasmissione bilanciata, separando i conduttori del segnale dai conduttori per schermatura e messa a terra, riduce la complessità del problema.

Oggi la maggior parte dei cavi (doppini) posati non sono schermati, fondamentalmente per ragioni di costo e di semplicità di installazione. In futuro è prevedibile che si faccia un maggior uso di schermi, sia per aumentare le prestazioni sia per ridurre i disturbi elettromagnetici generati dal cavo stesso.

3.2.5 Caratteristiche elettriche

I parametri meccanici finora descritti (materiali impiegati, schermature, geometrie) determinano i parametri elettrici del cavo stesso. La relazione tra di essi, tuttavia, non è esprimibile con formule semplici (e a volte neanche con formule complesse), soprattutto alle alte frequenze, dove, oltre ai fenomeni puramente elettrici, è necessario considerare anche i fenomeni elettromagnetici. Oggetto di questo paragrafo è la descrizione dei principali parametri elettrici.

L'*impedenza* è il parametro elettrico più importante per un cavo usato ad alte frequenze. L'impedenza, normalmente indicata con il simbolo *Z*, è espressa in ohm (Ω) ed è la somma di due componenti ($Z = R + jI$) in quanto sintetizza in un solo valore resistenze, capacità ed induttanze presenti sul cavo. Ciò che interessa analizzare non è tanto il valore nominale di impedenza ad una data frequenza, ma il variare di tale valore al variare della frequenza. Più l'impedenza è stabile al variare della frequenza, migliore è il cavo, e la presenza di schermi normalmente migliora tale aspetto. Oggi si certifica l'impedenza dei cavi nell'intervallo da 100 KHz a 350 MHz.

L'importanza dell'impedenza è dovuta al fatto che per la trasmissione di segnali a frequenze elevate l'impedenza di uscita del trasmettitore, l'impedenza di ingresso del ricevitore e l'impedenza caratteristica del cavo devono essere uguali (si parla di sistemi "adattati in impedenza"). Le variazioni di impedenza lungo il cavo, che nel caso di doppini possono essere provocate da alterazioni nella regolarità della geometria, provocano riflessioni del segnale, con conseguenti attenuazioni e interferenze. In passato si sono usati cavi per TD con impedenze comprese tra i 50 e i 150 Ω, oggi la maggior parte dei cavi ha una impedenza di 100 Ω.

La propagazione dei segnali elettrici non avviene istantaneamente, e per i segnali ad alta frequenza questo fenomeno diventa rilevante in quanto il trasmettitore può terminare di trasmettere l'informazione prima che il ricevitore abbia iniziato a riceverla. I parametri di funzionamento di alcuni protocolli di livello MAC per le LAN (ad esempio CSMA/CD, il protocollo della rete Ethernet 802.3) sono stati calcolati proprio sulla base di questo fenomeno.

Si definisce *velocità di propagazione* v_p la percentuale della velocità della luce nel vuoto (circa $3 \cdot 10^8$ m/s) alla quale si propaga un segnale elettrico sul cavo. Per i cavi in rame v_p varia tra il 55% e il 75%. Questo implica una velocità di propagazione dell'informazione di circa 200.000 Km/s. Anche se sembra una velocità elevata, va considerato che ad una velocità di trasmissione di 10 Mb/s, al termine del tempo dedicato alla trasmissione di un bit, il bit stesso ha percorso soltanto 20 m.

Altro importante parametro elettrico è l'*attenuazione*, che per i mezzi elettrici è definita come rapporto, in dB, della tensione del segnale in ingresso al cavo e la tensione misurabile all'altra estremità. L'attenuazione così misurata cresce linearmente con la lunghezza del cavo e con la radice quadrata della frequenza.

La *diafonia*, in inglese *cross-talk*, è invece la misura in dB di quanto un cavo disturba un altro cavo vicino. Spesso viene data come attenuazione di diafonia e quindi come parametro di merito (quanto è attenuato il segnale indotto da un cavo nel cavo vicino). In linea di principio esistono due modi diversi per misurare la diafonia: se la misura del segnale indotto nel cavo vicino è effettuata dalla stessa parte del trasmettitore si parla di paradiafonia o NEXT (*Near End Cross-Talk*, figura 3.14), se è effettuata all'estremo opposto di parla di telediafonia o FEXT (*Far End Cross-Talk*, figura 3.15).

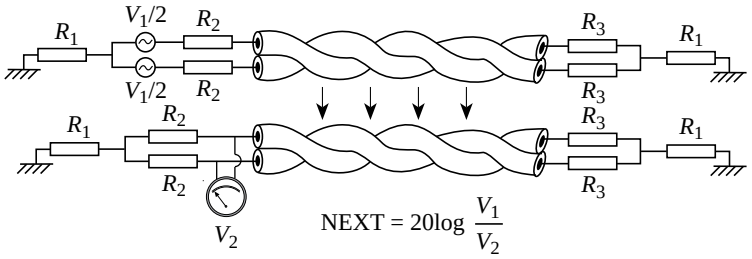


Fig. 3.14 - Schema di misura della paradiafonia (NEXT).

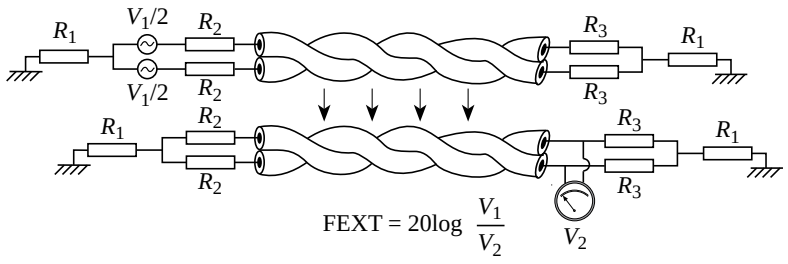


Fig. 3.15 - Schema di misura della telediafonia (FEXT).

In pratica, si misura quasi sempre soltanto la paradiafonia (NEXT), indicandola con il nome generico di diafonia. Infatti nella trasmissione su due coppie, una in trasmissione ed una in ricezione, il valore della telediafonia non interessa, in quanto all'estremità considerata dalla misura non si trova un ricevitore bensì il trasmettitore dell'altra coppia. Inoltre, per la misura del NEXT, è sufficiente un unico strumento comprendente generatore di segnale e misuratore di tensione collegato ad una sola estremità del cavo. La semplicità e rapidità delle operazioni di misura dei parametri elettrici dei cavi installati è di fondamentale importanza, ad installazione terminata, nella certificazione della qualità dei sistemi di cablaggio.

Le misure di telediafonia e paradiafonia sono inevitabilmente affette dall'attenuazione introdotta dal cavo. È interessante notare che per quanto riguarda il NEXT, le parti di cavo più lontane dal generatore di segnale portano un contributo via via inferiore; infatti il segnale iniettato è attenuato, e il segnale indotto nella coppia vicina deve ancora essere attenuato altrettanto prima di giungere allo strumento di misura. Ne segue che, a partire da una certa distanza, i contributi diventano trascurabili. Sperimentalmente si osserva che il NEXT cresce molto al crescere della lunghezza del cavo per i primi metri, poi si stabilizza ad un valore massimo pressoché indipendente dalla lunghezza.

La diafonia è un parametro particolarmente importante nei doppini, in quanto più coppie scorrono affiancate all'interno della stessa guaina.

Ai fini di una corretta ricezione non interessano tanto l'attenuazione assoluta del cavo o il suo valore di diafonia, quanto la combinazione di questi due parametri. Infatti, se si considera trascurabile il rumore indotto dall'esterno, è tale combinazione che determina il rapporto segnale/rumore in ingresso al ricevitore, e quindi l'integrità del segnale. Esiste un parametro che rappresenta le due grandezze in modo combinato: l'ACR (*Attenuation to Cross-talk Ratio*), che esprime il rapporto tra il segnale attenuato presente su una coppia ed il segnale indotto dalla coppia

vicina. Esso varia in funzione della frequenza e della lunghezza del cavo. La figura 3.16 illustra il caratteristico andamento della diafonia e dell'attenuazione, ad una certa frequenza, al variare della lunghezza di un cavo. Siccome attenuazione e diafonia sono espresse in dB, cioè in termini logaritmici, il loro rapporto è ottenibile come differenza tra tali valori, e quindi nella figura l'ACR è la distanza tra le curve. Quando questa distanza è troppo ridotta non è più possibile trasmettere sul cavo in modo affidabile in quanto il segnale è troppo debole rispetto al rumore e quindi possono verificarsi troppi errori di trasmissione.

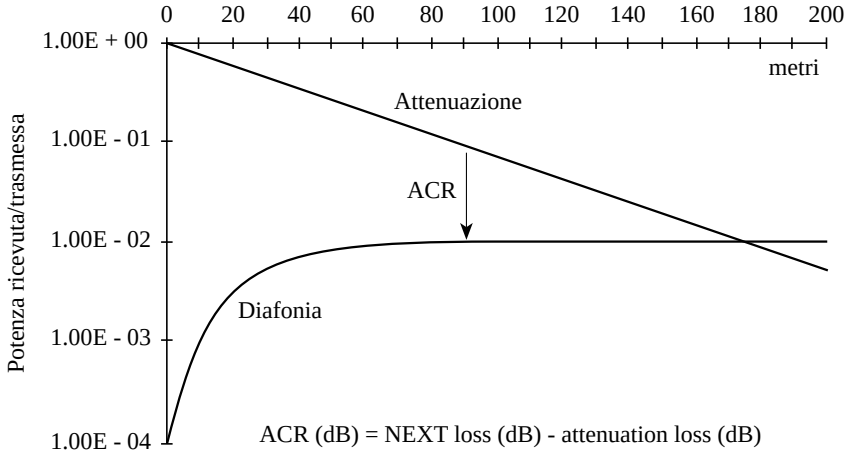


Fig. 3.16 - ACR, attenuazione e diafonia..

Le irregolarità nella geometria del cavo generano variazioni nell'impedenza caratteristica. Quando un segnale elettrico, propagandosi lungo il cavo, incontra tali discontinuità viene totalmente o parzialmente riflesso, riducendo l'energia del segnale trasmesso. La perdita per riflessione di un cavo è definita dal parametro *structural return loss*, o semplicemente *return loss*, ed è misurata in dB. Inoltre, nel caso dei doppini le irregolarità nella geometria comportano pressoché sempre delle asimmetrie nelle coppie, e parte dei disturbi elettromagnetici che dovrebbero interessare in egual misura i due conduttori (rumore "longitudinale") generano una componente differenziale, che non può essere eliminata dal ricevitore. Esistono due parametri che definiscono tale caratteristica delle linee bilanciate: il *longitudinal to differential conversion loss* (anche *balance*, bilanciamento), misurato dalla parte del trasmettitore, e il *longitudinal conversion transfer loss*, misurato dalla parte del ricevitore. Il primo determina quanto disturbo elettromagnetico irradierà il cavo, il secondo quanto rumore arriverà al ricevitore.

3.2.6 I compromessi nella realizzazione dei mezzi trasmissivi elettrici

Un mezzo trasmissivo elettrico *ideale*, che trasporti tutta l'energia del segnale trasmesso senza attenuazione né distorsione, non esiste.

Un mezzo trasmissivo elettrico *ottimale* è caratterizzato da bassa resistenza, bassa capacità e bassa induttanza, cioè è un mezzo poco dispersivo e poco dissipativo. In tale mezzo quasi tutta la potenza inviata sul canale dal trasmettitore arriva al ricevitore ed il segnale non viene distorto. Un tale cavo dovrebbe avere elevata dimensione del conduttore interno, buona spaziatura tra i conduttori, bassa costante dielettrica dell'isolante (al limite quella dell'aria) e schermatura individuale delle coppie e globale del cavo. Ne risulterebbe un cavo ingombrante, pesante, difficile da posare e facilmente incendiabile; invece le esigenze pratiche per un'agevole installazione indicano la flessibilità, la resistenza alla trazione e il rispetto delle varie normative di sicurezza. Perciò la scelta cade sempre su un compromesso subottimale.

3.2.7 Il cavo coassiale

Il cavo coassiale (figura 3.17) ha avuto per lungo tempo notevole diffusione nelle reti locali; per esempio è stato utilizzato in due diverse versioni dello standard 802.3 (Ethernet) e per il collegamento di terminali IBM. Ora è caduto in disuso nelle LAN, eliminato dallo standard ISO/IEC 11801 per i cablaggi strutturati e sostituito dalle fibre ottiche nella fascia ad alte prestazioni e dai doppini in quella a medie prestazioni, mentre continua ad essere utilizzato nelle reti geografiche.

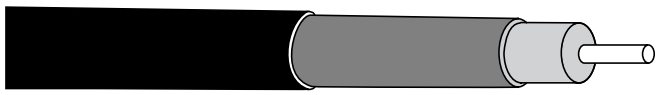


Fig. 3.17 - Cavo coassiale.

Un cavo coassiale è formato da un conduttore centrale e da uno o più schermi (calze, fogli); per la trasmissione di segnali ad alta frequenza il trasmettitore, il cavo e il ricevitore devono costituire un sistema adattato in impedenza. La coassialità dei conduttori e la schermatura che il conduttore esterno offre nei confronti di quello interno rendono il cavo coassiale più immune ai disturbi elettromagnetici rispetto ai doppini non schermati; tuttavia, come già visto nel paragrafo 3.2.3, ogni eventuale corrente di disturbo che scorre lungo lo schermo

determina un'alterazione del valore della tensione di riferimento che può provocare errori nella ricezione del segnale.

Il cavo coassiale è stato soppiantato dal doppino per diverse ragioni. Tra queste:

- maggior costo, sia dei materiali (soprattutto i connettori), sia per la maggior difficoltà di installazione;
- maggior ingombro: un cavo per Ethernet 10Base2 trasporta un singolo segnale ed occupa circa lo stesso spazio di un cavo TP a quattro coppie, che può trasportare quattro segnali;
- minor flessibilità: il cavo coassiale è adatto soltanto ad alcuni servizi, quali LAN o televisione via cavo, mentre per numerosi altri, quali telefoni, citofoni, apriporta, controllo accessi, ecc., è previsto soltanto l'utilizzo del doppino. Questo aspetto, forse il più importante, verrà approfondito nel capitolo dedicato ai cablaggi strutturati.

Come esempio vediamo il cavo *thick Ethernet* (RG213) in figura 3.18, caratterizzato da ottimi parametri elettrici (si osservi la schermatura a quattro strati), ma costoso, difficile da porre in opera e con notevoli problemi legati ai raggi minimi di curvatura ammessi.

Fig. 3.18 - Cavo Thick Ethernet.

L'unico tipo di cavo coassiale che trova ancora una qualche utilizzazione è il *thin Ethernet* (figura 3.19), per lo standard IEEE 802.3 10Base2. Spesso al suo posto è anche utilizzato il più comune RG58, che anziché avere un doppio schermo (foglio più calza) dispone di uno schermo singolo (calza).

Fig. 3.19 - Cavo Thin Ethernet.

La fase di transizione dall'uso del cavo coassiale all'uso del doppino è stata lenta e graduale, e in molte realtà è tuttora in corso. Di conseguenza, molti servizi prevedono ancora il cavo coassiale, e anche per quelli per i quali sono già stati emanati nuovi standard per il doppino, resta il problema del recupero delle apparecchiature già in possesso dell'utenza e perfettamente funzionanti nel momento in cui devono essere installate su una infrastruttura di cablaggio che non prevede il cavo coassiale. La conversione da doppino (su cui si usa la trasmissione bilanciata) a coassiale (su cui si usa la trasmissione sbilanciata) e viceversa può essere ottenuta con i cosiddetti *balun* (*BALanced to UNbalanced*). I balun possono essere passivi, cioè realizzati con piccoli trasformatori (figura 3.20), oppure attivi, realizzati con dispositivi elettronici che richiedono alimentazione elettrica e che spesso determinano caratteristiche migliori rispetto ai balun passivi. I balun possono essere montati direttamente all'interno di appositi connettori.

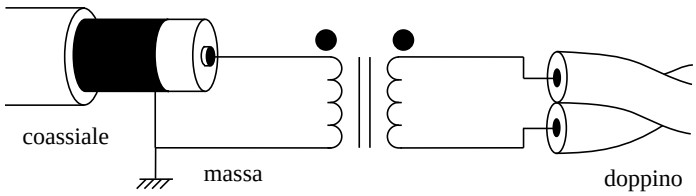


Fig. 3.20 - Balun.

3.2.8 Il doppino

Il doppino è il mezzo trasmissivo classico della telefonia e consiste in due fili di rame ricoperti da una guaina isolante e ritorti (o "binati" o "twisted") detti comunemente "coppia" (*pair*, in inglese, da cui *twisted pair* o *TP*). Il tipo di doppino più usato attualmente ha un diametro di 24 AWG e un'impedenza di 100 Ω (figura 3.21).

Fig. 3.21 - Doppino di rame.

La binatura serve a ridurre i disturbi elettromagnetici come spiegato nel

paragrafo 3.2.3. Normalmente si utilizzano cavi con più coppie (4, 25, 50 e oltre) ed è allora necessario adottare passi di binatura differenziati da coppia a coppia per ridurre la diafonia tra le coppie. Infatti, se i passi di binatura fossero uguali, ogni conduttore di una coppia si troverebbe sistematicamente affiancato, ad ogni spira, con uno dei due conduttori dell'altra coppia, e quindi verrebbe a cadere l'ipotesi di perfetta simmetria della trasmissione bilanciata. I campi elettromagnetici generati dalle due coppie interferirebbero reciprocamente con un considerevole peggioramento della diafonia.

I doppini sono nati come mezzo trasmissivo a banda molto ridotta (la banda fonica usata nella telefonia è inferiore a 4 KHz), ma negli ultimi anni hanno raggiunto prestazioni una volta raggiungibili soltanto con i cavi coassiali. I miglioramenti sono stati ottenuti realizzando nuovi materiali isolanti, curando la geometria delle coppie (anche tramite l'adozione di particolari guaine esterne), mettendo a punto sofisticati algoritmi di differenziazione dei passi di binatura e aumentando la sezione dei conduttori. Attualmente i doppini possono competere nelle medie velocità (10 - 100 Mb/s) e sulle brevi distanze (inferiori a 100 m) con le fibre ottiche.

Le caratteristiche che hanno tuttavia inciso maggiormente sulla diffusione del doppino sono la compatibilità con la telefonia e la facilità di posa in opera (la connettorizzazione a perforazione di isolante è semplice, veloce ed economica, anche se alle alte velocità rappresenta un elemento critico, in quanto è il punto in cui le coppie devono essere per forza sbinate).

Esistono varie versioni di doppino:

- STP (*Shielded Twisted Pair*), versione con uno schermo per ogni coppia più uno schermo globale;
- *Screened*, FTP (*Foiled Twisted Pair*) o S-UTP (figura 3.22), versione con un unico schermo (normalmente in foglio di alluminio) per tutto il cavo;
- UTP (*Unshielded Twisted Pair*) (figura 3.23) versione non schermata.

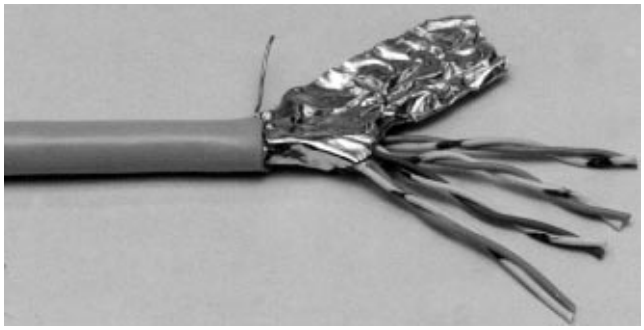


Fig. 3.22 - Doppino FTP.

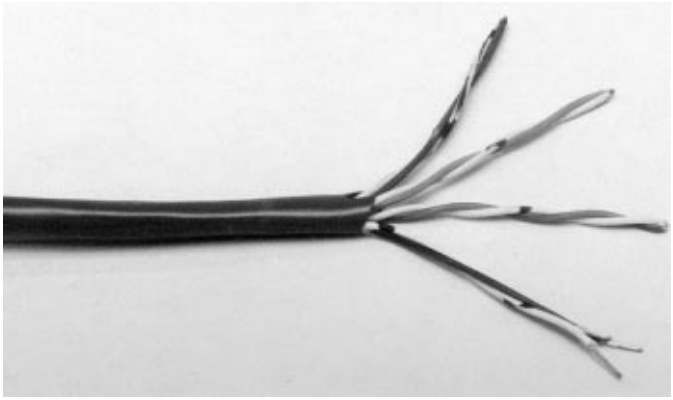


Fig. 3.23 - Cavo UTP.

Gli schermi possono essere dei tipi precedentemente descritti (a foglio, a calza o entrambi).

Il tipo più semplice di doppino è un UTP con binatura minima di 6 giri/metro, impedenza di 100 Ω (+/- 15%) da 1 a 16 MHz e attenuazione massima, per una tratta lunga 100 m, di 10 dB tra 5 e 10 MHz. Il doppino più diffuso, soprattutto per collegare le prese utente, è UTP a quattro coppie da 24 AWG.

Alcuni costruttori hanno sempre adottato doppini schermati (STP); in particolare, IBM ha sviluppato una serie di cavi ad altissime prestazioni, ma di elevato ingombro e per questo difficili da posare. In figura 3.24 è illustrato il cavo IBM "tipo 1" pensato appositamente per la rete locale IBM Token Ring. Si tratta di un STP a 150 Ω dotato unicamente di due coppie singolarmente schermate.

Fig. 3.24 - Cavo "tipo 1" IBM.

Esso non è idoneo a collegare utenze di tipo telefonico in quanto ha un numero di coppie insufficiente, un valore di impedenza errata e un costo eccessivo per un servizio a così basse prestazioni. Quando si vogliono soddisfare tali utenze occorre

installare il cavo IBM "tipo 2" che contiene un cavo "tipo 1" più quattro coppie a 100 Ω per la telefonia. Attualmente IBM produce un nuovo sistema di cablaggio chiamato *ACS* (*Advanced Connectivity System*) che fa uso di cavi FTP o UTP di categoria 5 (si veda il paragrafo 3.2.9) a 100 Ω, 24 AWG.

Nella tabella 3.3 sono riportate le caratteristiche di un cavo FTP (Belden 1456A), di un UTP (AT&T 2061), del "tipo 1" e del "tipo 2" IBM. Si notino, oltre alle variazioni di attenuazione e diafonia, anche la dimensione e il peso.

Caratteristica	Belden 1456A	AT&T 2061	IBM Tipo1	IBM Tipo2
AWG	24	24	22	22
Z	100 Ω	100 Ω	150 Ω	150 Ω
Velocità di propagazione	66 %	non dichiarata	81 %	81 %
C	52.5 nF/Km	52 nF/Km	29 nF/Km	29 nF/Km
F (esterno)	5.6 mm	4.3 mm	9.5 mm	11 mm
Peso	39 Kg/Km	27 Kg/Km	91 Kg/Km	138 Kg/Km
Attenuazione (100m)	6.6 dB a 10 MHz	6.5 dB a 10 MHz	2.2 dB a 4 MHz	2.2 dB a 4 MHz
Attenuazione (100m)	8.3 dB a 16 MHz	8.1 dB a 16 MHz	4.5 dB a 16 MHz	4.5 dB a 16 MHz
Cross-talk (100m)	42 dB a 10 MHz	47 dB a 10 MHz	58 dB a 5 MHz	58 dB a 5 MHz
Cross-talk (100m)	40 dB a 16 MHz	44 dB a 16 MHz	40 dB a 20 MHz	40 dB a 20 MHz

Tab. 3.3 - Caratteristiche di cavi TP.

3.2.9 Classificazione dei doppini

I parametri elettrici di qualsiasi cavo variano al variare della frequenza. Occorre pertanto chiedersi, per una data applicazione, a quale frequenza sia opportuno analizzare i parametri per decidere se un cavo sia adeguato all'applicazione stessa. Questo dipende dalla codifica fatta a livello fisico (si veda il paragrafo

3.1.2), e dovendo valutare l'utilizzabilità di un cavo, bisogna analizzarne le caratteristiche elettriche in corrispondenza della frequenza fondamentale di trasmissione utilizzata dallo standard di rete locale scelto. Viceversa, dovendo realizzare un'infrastruttura di trasmissione di segnali, e quindi installare cavi adatti a più applicazioni, sarebbe necessario considerare un elevato numero di valori dei parametri elettrici, a tutte le frequenze interessate dalle possibili applicazioni. Per evitare questa operazione si è ricorso ad una classificazione dei cavi di uso più comune, cioè dei doppini. Tale classificazione prevede cinque *categorie*, in base alle applicazioni per le quali i cavi sono idonei. La categoria 1 è quella dei cavi peggiori, la 5 quella dei cavi migliori. Ogni categoria è inoltre idonea a fornire tutti i servizi offerti dalle categorie inferiori.

- La categoria 1 (*Telecommunication*) comprende i cavi adatti unicamente a telefonia analogica.
- La categoria 2 (*Low Speed Data*) comprende i cavi per telefonia analogica e digitale (ISDN) e trasmissione dati a bassa velocità (per esempio linee seriali).
- La categoria 3 (*High Speed Data*) è la prima categoria di cavi adatti a realizzare reti locali fino a 10 Mb/s, in particolare per soddisfare gli standard 10BaseT di 802.3 e Token-Ring a 4Mb/s.
- La categoria 4 (*Low Loss, High Performance Data*) comprende i cavi per LAN Token-Ring fino a 16 Mb/s.
- La categoria 5 (*Low Loss, Extended Frequency, High Performance Data*) comprende i migliori cavi disponibili, per applicazioni fino a 100 Mb/s, su distanze di 100 metri.

Ogni categoria è definita da un insieme di parametri elettrici, alcuni dei quali, fortemente dipendenti dalla frequenza, come attenuazione e diafonia, sono espressi in termini di punti di una curva per diversi valori di frequenza. Proprio le curve di attenuazione e la diafonia variano moltissimo al variare della categoria. In particolare, al crescere della categoria e a parità di frequenza, la curva di attenuazione diminuisce sempre più la sua pendenza tendendo a divenire orizzontale, mentre la curva di diafonia si abbassa. La tabella 3.4 riporta le caratteristiche principali, compresa l'attenuazione, per le tre categorie di interesse per le LAN; la tabella 3.5 riporta i dati relativi alla diafonia (NEXT). Relativamente a quest'ultima, occorre notare che, a causa della progressione non lineare in funzione della distanza, dovuta alla misura effettuata dal lato del trasmettitore, i valori rimangono pressoché invariati quando sono riferiti a distanze maggiori o uguali a 100 metri.

Caratteristiche del cavo			Categoria del cavo		
Caratteristiche elettriche @ 20 °C	Unità di misura	MHz	3	4	5
Impedenza	Ω	1–16 1–20 1–100	100 +/– 15%	100 +/– 15%	100 +/– 15%
Mutua capacità di ogni coppia	nf/100 m	0.1	6.57	5.59	5.59
Velocità di propagazione			0.6 c	0.6 c	0.6 c
Massimo valore di resistenza	Ω/100 m		9.4	9.4	9.4
Attenuazione massima ammessa	dB/100 m	0.064 0.256 0.512 0.772 1 4 8 10 16 20 25 31.25 62.5 100	0.92 1.31 1.84 2.23 2.56 5.59 8.55 9.86 13.15 - - - - -	0.75 1.11 1.51 1.87 2.13 4.27 6.25 7.23 8.88 10.2 - - - -	0.72 1.05 1.48 1.81 2.07 4.27 5.92 6.57 8.22 9.21 10.52 11.84 17.11 22.04

Tab. 3.4 - Caratteristiche dei cavi di categoria 3, 4, 5.

I cavi di categoria 5 rappresentano oggi lo stato dell'arte nel campo del cablaggio delle LAN. Dalle tabelle 3.4 e 3.5 si nota che, fino alla frequenza di 100 MHz, il valore di ACR non scende quasi mai sotto i 10 dB (nel caso peggiore 32 - 22.04 = 9.96 dB). Tutti gli standard di rete a velocità di 100 Mb/s o maggiori con trasmissione su due coppie prevedono l'uso di cavi di categoria 5. Tuttavia, poiché gli standard per i cablaggi strutturati impongono la posa di doppini a 4 coppie per ogni presa, alcuni recenti standard per LAN a 100 Mb/s prevedono l'utilizzo di tutte e quattro le coppie, suddividendo su di esse la trasmissione dei dati. Questo riduce la banda necessaria, e consente di operare su cavi di categoria 3.

Caratteristiche del cavo			Categoria del cavo		
Caratteristiche elettriche @ 20 °C	Unità di misura	MHz	3	4	5
Near End Crosstalk (NEXT), minimo valore ammesso	dB @ 100 m	0.150	54	68	74
		0.772	43	58	64
		1	41	56	62
		4	32	47	53
		8	28	42	48
		10	26	41	47
		16	23	38	44
		20	-	36	42
		25	-	-	41
		31.25	-	-	40
		62.5	-	-	35
		100	-	-	32

Tab. 3.5 - Diafonia dei cavi di categoria 3, 4, 5.

3.2.10 Doppini di nuova generazione

Sul mercato sono attualmante presenti molti cavi omologati in categoria 5 e alcune ditte hanno già prodotto cavi con prestazioni notevolmente superiori.

La Belden, ad esempio, ha sviluppato e realizzato un cavo UTP innovativo chiamato *DataTwist 350* che migliora principalmente le caratteristiche di attenuazione, diafonia tra le coppie e regolarità dell'impedenza rispetto ad un normale cavo di categoria 5. La novità introdotta consiste nel ricavare i due fili costituenti una coppia da un'unica estrusione di materiale isolante, per cui si ottiene una concentricità quasi perfetta tra il conduttore centrale e l'isolante. Inoltre gli isolanti dei due conduttori rimangono saldati e si evita quindi la presenza irregolare di aria che altererebbe le caratteristiche elettriche e la geometria. Questa particolare tecnica costruttiva permette di mantenere pressoché inalterate le caratteristiche elettriche del cavo anche ad installazione avvenuta. Come conseguenza, le caratteristiche elettriche, rispetto alla categoria 5, risultano così migliorate:

- l'impedenza è quasi costante lungo tutto il cavo, il valore è mantenuto in una tolleranza del 15 % rispetto al valore nominale nelle frequenze tra 1 e 100 MHz, ed in una tolleranza del 20 % nelle frequenze tra 100 e 350 MHz;

- l'attenuazione a 100 MHz, su una lunghezza di 100 m, è inferiore di circa 2 dB;
- la diafonia tra le coppie (NEXT) è migliorata di circa 4 dB;
- il valore di ACR a 100 MHz è migliorato di circa 6 dB.

Un altro esempio è dato dalla Montrose che ha realizzato un cavo FTP innovativo chiamato *Languard 200*, in cui sono stati curati particolarmente gli aspetti della schermatura globale e dell'assemblaggio del cavo, in modo da ottenere delle ottime caratteristiche elettriche e ridurre l'emissione di radio frequenze. Lo schermo è costituito da un foglio di alluminio dello spessore di 0.15 mm e da una calza di rame dello spessore di 0.1 mm. Le caratteristiche costruttive di questo cavo migliorano i valori di impedenza, attenuazione e soprattutto di diafonia tra le coppie, rispetto ad un normale cavo di categoria 5:

- l'impedenza è quasi costante lungo tutto il cavo, il valore è mantenuto in una tolleranza del 12 % rispetto al valore nominale nelle frequenze tra 1 e 100 MHz ed in una tolleranza del 15 % nelle frequenze tra 100 e 200 MHz;
- l'attenuazione a 100 MHz, su una lunghezza di 100 m, è inferiore di circa 1 dB;
- la diafonia tra le coppie (NEXT) è migliorata di circa 11 dB;
- il valore di ACR a 100 MHz è migliorato di circa 12 dB.

3.3 LE FIBRE OTTICHE

L'idea di utilizzare la luce come mezzo di comunicazione risale a circa 200 anni fa. Nel 1790 Claude Chappe costruì un telegrafo ottico composto da torri equipaggiate con braccia mobili. Tuttavia, per trovare qualche applicazione pratica bisogna giungere al 1953 quando Kapany mise a punto fibre ottiche di vetro con le quali, qualche anno dopo, insieme ad Hopkins, realizzò i primi endoscopi a fibra ottica.

Il rallentamento dello sviluppo e dell'impiego delle fibre ottiche era dovuto all'elevata attenuazione, che nel 1965 raggiungeva ancora i 1000 dB/Km. Soltanto nel 1967 è stato possibile affermare che le fibre ottiche hanno la potenzialità di rivoluzionare le comunicazioni sostituendo il cavo metallico. Infatti in quegli anni fu individuata la causa delle elevate attenuazioni nella non sufficiente purezza del materiale utilizzato. Nel 1970 si assistette ad una svolta storica: i ricercatori della Corning Glass Works riuscirono a perfezionare una fibra ottica con attenuazione di "soli" 20 dB/Km alla lunghezza d'onda di 633 nm (nanometri, 10^{-9}m).

I progressi sono poi stati rapidi: nel 1972 una fibra graded index raggiungeva

un'attenuazione di 4 dB/Km e ai nostri giorni valori di 0.2 dB/Km a 1550 nm sono raggiunti dalle fibre monomodali. Anche la tecnologia dei trasmettitori e dei ricevitori per fibra ottica ha compiuto grandi passi in avanti in termini di potenza, sensibilità e durata dei dispositivi.

Per quanto concerne lo sfruttamento delle fibre ottiche, i primi cavi sono diventati operativi tra il 1973 e il 1976. La fine degli anni ottanta ha segnato la maturità delle fibre ottiche, e a partire dall'inizio degli anni novanta esse sono state impiegate anche per le reti locali.

3.3.1 Fisica delle fibre ottiche

Il vetro, se stirato a dimensioni micrometriche, perde la sua caratteristica di fragilità e diventa un filo flessibile e robusto. Una fibra ottica si presenta come un sottile filo di materiale vetroso costituito da due parti (figura 3.25): la più interna prende il nome di nucleo (*core*), e l'esterna di mantello (*cladding*). Il core ed il cladding hanno indici di rifrazione diversi, ed il primo è più denso del secondo. La differenza negli indici di rifrazione determina la possibilità di mantenere la luce totalmente confinata all'interno del core.

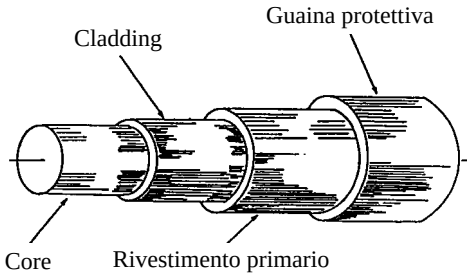


Fig. 3.25 - Fibra ottica.

Il grande successo delle fibre ottiche è dovuto a diversi fattori tra cui:

- totale immunità da disturbi elettromagnetici, non impiegando materiali conduttori, e trasportando particelle (fotoni) elettricamente neutri;
- alta capacità trasmissiva: sono operative fibre ottiche a 2 Gb/s;
- bassa attenuazione: alcuni decimi di dB/Km;
- dimensioni ridottissime e costi contenuti.

Per contro, le fibre ottiche sono unicamente adatte a collegamenti punto-punto, non essendo possibile prelevare o inserire il segnale in un punto intermedio, cosa invece possibile con mezzi trasmissivi elettrici.

La dimensione standard del diametro delle fibre è di 125 μm, e con il rivestimento esterno si giunge a diametri di circa 0.25 mm.

Le guaine protettive possono essere di due tipi, *tight* e *loose*, l'una aderente e solidale con la fibra, l'altra lasca, praticamente un tubicino di plastica in cui è inserita la fibra. Inoltre, le fibre possono essere raggruppate come nelle cosiddette *slotted core*, caratterizzate dalla presenza di un elemento centrale in vetroresina cui è collegata una struttura a scanalature sulla quale vengono poggiati gruppi di fibre (di solito quattro). Per una descrizione più accurata dei cavi in fibra ottica si veda il paragrafo 3.3.2.

Le proprietà e i modi di propagazione dell'energia luminosa in una fibra ottica possono essere studiati mediante la teoria delle guide d'onda. Un'analisi semplificata, ma precisa sino a quando le dimensioni della fibra sono molto maggiori di quelle della lunghezza d'onda, può essere effettuata applicando le leggi dell'ottica geometrica. La legge di Snell (figura 3.26), in particolare, studia la riflessione e la rifrazione di un raggio luminoso incidente sulla superficie di separazione di due materiali. Essa dimostra che per valori dell'angolo di incidenza superiori a $\alpha_c = \sin^{-1}(n_2/n_1)$, detto angolo critico, si ha riflessione totale. Nelle fibre ottiche valori tipici per gli indici di rifrazione sono n_2=1.475 per il cladding e n_1=1.5 per il core. Pertanto, $\alpha_c \cong 79.5$ gradi.

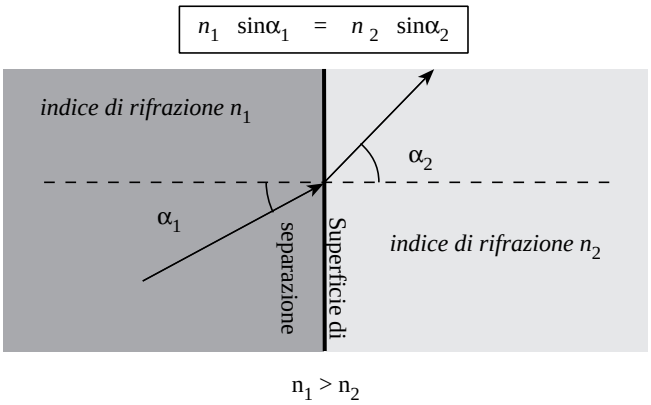


Fig. 3.26 - Legge di Snell.

Perché fra il core e il cladding avvenga la riflessione totale dei raggi luminosi è necessario che essi siano introdotti ad una estremità ottica entro un certo angolo di accettazione della fibra. Tanto maggiore sarà l'angolo di accettazione tanto più alta sarà la cosiddetta apertura numerica (NA) della fibra, cioè la quantità di luce che si riesce ad introdurre (figura 3.27). Con i valori dell'esempio precedente risulta NA = 0.18.

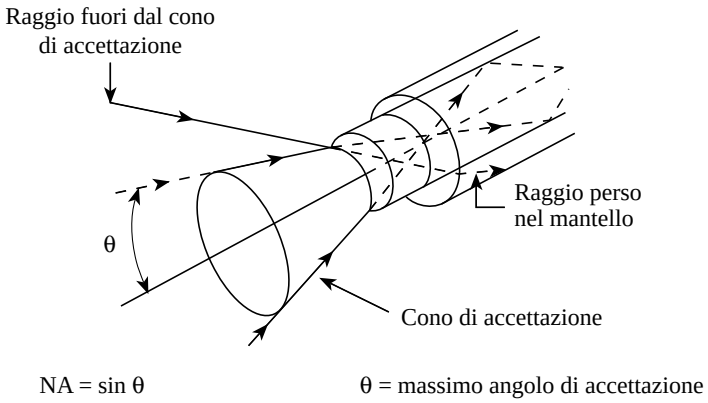


Fig. 3.27 - Cono di accettazione.

Esistono però anche altri aspetti che regolano la propagazione della luce nella fibra ottica e che rendono necessario prendere in considerazione anche altri fattori, specificati meglio nelle equazioni di Maxwell. Dalla soluzione di queste equazioni si ricava che l'energia si propaga nella fibra in un numero discreto di configurazioni. Queste configurazioni sono chiamate *modi* e ogni singolo modo ha sue caratteristiche di propagazione.

Le fibre ottiche che ammettono più modi di propagazione vengono dette multimodali. La fibra ottica multimodale più diffusa è la 62.5/125: il primo numero indica il diametro del core in μm (micron, 10^{-6}m), il secondo quello del cladding.

Nelle fibre ottiche multimodali i raggi che si propagano secondo i diversi modi percorrono cammini di lunghezza diversa, cui corrispondono tempi di propagazione diversi. Questo fenomeno si chiama dispersione modale e pone un limite inferiore alla durata minima di un impulso luminoso, limitando quindi la velocità di trasmissione. Infatti, se alimentiamo la fibra ottica con un impulso luminoso molto breve (di durata T1) notiamo che al suo arrivo all'estremità opposta (figura 3.28) l'impulso si presenta deformato (di durata T2).

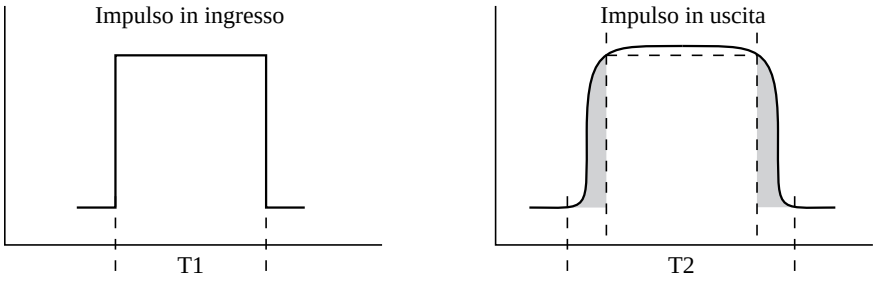


Fig. 3.28 - Dispersione modale.

Le fibre multimodali si dividono, a seconda del profilo radiale dell'indice di rifrazione, in fibre *step-index* (figura 3.29) e fibre *graded-index* (figura 3.30).

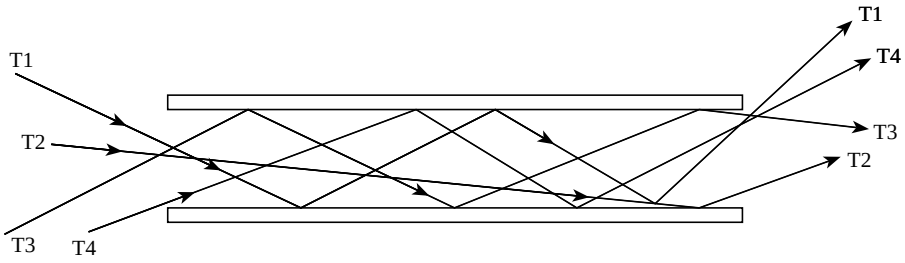


Fig. 3.29 - Fibra step-index.

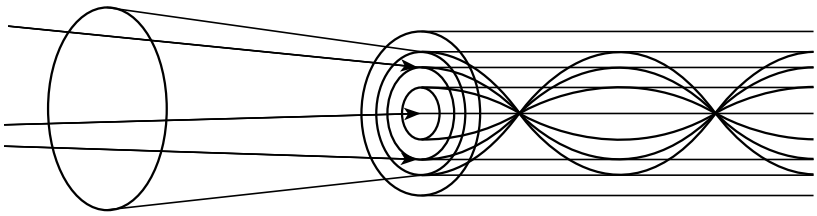


Fig. 3.30 - Fibra graded-index.

Le fibre step-index sono caratterizzate da un indice di rifrazione costante fra il centro e la periferia del core. L'indice di rifrazione decresce bruscamente con un gradino (step) entrando nel cladding.

Nelle fibre ottiche a profilo d'indice graduale o graded-index, il profilo d'indice di rifrazione varia gradualmente lungo il diametro della fibra, passando da un valore massimo al centro del core e decrescendo gradualmente sino ad assumere un valore minimo al confine fra core e cladding.

Il fenomeno della dispersione modale è molto più accentuato nelle fibre step-index rispetto alle fibre graded-index. Infatti nelle prime i raggi luminosi hanno un andamento tipicamente a zig-zag e compiono percorsi di lunghezza anche molto diversa a velocità costante. Nelle fibre graded-index, invece, si sfrutta il fenomeno per cui la velocità di propagazione della luce è inversamente proporzionale all'indice di rifrazione del mezzo. Tarando opportunamente il profilo radiale dell'indice di rifrazione per diminuire la velocità dei raggi che hanno cammino più breve (quelli centrali), si può ridurre la dispersione modale.

Valori tipici di banda passante delle fibre multimodali sono 22 MHz · Km per le fibre step-index e 1GHz · Km per quelle graded-index.

La soluzione definitiva al problema della dispersione modale è quella di ridurre fortemente (fino a 8-10 μm) la dimensione del core, per consentire la propagazione dei raggi di un solo modo (figura 3.31).

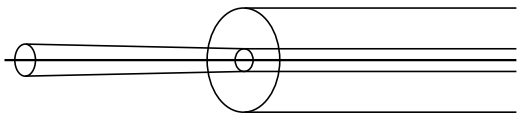


Fig. 3.31 - Fibra monomodale.

Si ottengono così fibre con cono di accettazione molto ridotto, dette *monomodali*, nelle quali la fibra ottica si comporta come una guida d'onda ammettendo una sola modalità propagativa. Bisogna però tenere in considerazione la dispersione cromatica, dovuta alla presenza di raggi a diversa lunghezza d'onda (e quindi di diversi colori, trattandosi di luce); per questo, mentre sulle fibre multimodali si può trasmettere mediante normali LED (ad ampio spettro di emissione), in quelle monomodali occorre utilizzare dei laser, più sofisticati e costosi, ma più precisi (con emissione di luce monocromatica e coerente). Evitando le dispersioni multimodale e cromatica si può trasmettere a velocità superiori e su distanze più lunghe.

Le fibre ottiche sono difficili da giuntare e da connettorizzare a causa delle loro esigue dimensioni che impongono precisioni notevoli. Tale difficoltà aumenta al diminuire delle dimensioni e quindi è più sentita nelle fibre ottiche monomodali (figura 3.32).

In particolare è più difficile connettorizzare le fibre che giuntarle, per cui molto spesso la connettorizzazione viene effettuata esclusivamente in laboratorio, mentre in campo ci si limita ad effettuare giunte con apposite macchine giuntatrici.

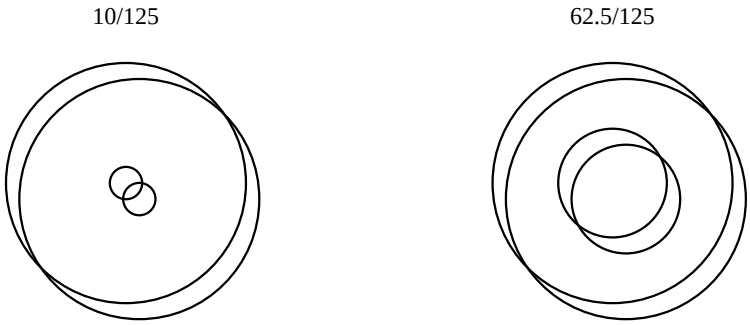


Fig. 3.32 - Interconnessione di due fibre ottiche.

La difficoltà di effettuare giunzioni e connettorizzazioni implica costi rilevanti, poiché è richiesto personale qualificato con strumentazione adeguata. Tali costi sono particolarmente alti per le fibre monomodali che richiedono precisioni estremamente elevate. Per questa ragione nelle reti locali si privilegia l'adozione di fibre multimodali più semplici da posare in opera. D'altra parte, le ridotte distanze da coprire rendono meno rilevanti i vantaggi delle fibre monomodali rispetto alle multimodali. L'alto costo di connettorizzazione limita inoltre l'impiego delle fibre ottiche alla realizzazione di dorsali di rete, mentre per collegare il singolo posto di lavoro il doppino di rame ha un miglior rapporto prestazione/prezzo. Per superare tali limiti sono allo studio fibre plastiche con diametro di 1 mm, che dovrebbero avere un basso costo di connettorizzazione e risultare competitive con i cavi in rame per il cablaggio dei posti di lavoro.

Un altro parametro delle fibre ottiche estremamente importante è l'attenuazione. Essa può essere espressa in funzione della lunghezza d'onda, ottenendo un grafico simile a quello di figura 3.33. Vi si individuano tre minimi di attenuazione in corrispondenza di tre intervalli di lunghezza d'onda, detti finestre. Le finestre corrispondono a tre tipi di utilizzazioni diverse: per la prima si usano solo LED comuni, per la seconda LED comuni e laser, per la terza solo laser.

Le lunghezze d'onda che interessano le comunicazioni ottiche sono quelle comprese tra i 750 nm ed i 1600 nm, cioè nel vicino infrarosso, in quanto le radiazioni visibili all'occhio umano vanno dai 455 nm (violetto) ai 750 nm (rosso).

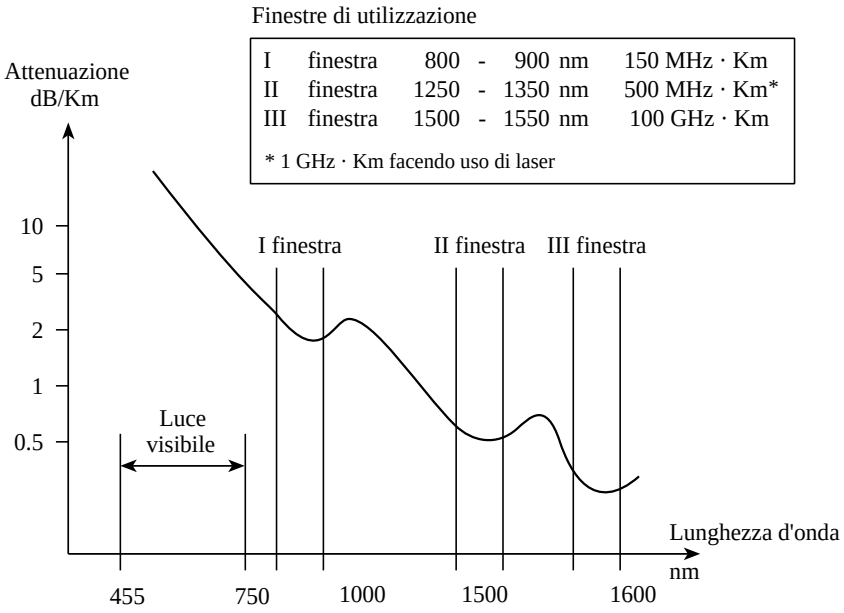


Fig. 3.33 - Finestre di utilizzo.

La prima finestra è collocata intorno agli 850 nm ed è stata la prima ad essere usata per la realizzazione di sistemi di trasmissione su fibra ottica. Essa è presente solo nella fibra multimodale.

La seconda finestra è posta a 1300 nm ed essendo caratterizzata da una attenuazione inferiore, è quella attualmente utilizzata per esigenze di bande passanti medie o alte. Essa è presente sia nella fibra multimodale sia in quella monomodale. La banda passante varia in funzione del tipo di fibra e del tipo di emettitore/ricevitore utilizzato, e può essere di:

- 500 MHz · Km, se si usano i LED su fibra multimodale;
- 1 GHz · Km, se si usano i laser su fibra multimodale;
- da decine a centinaia di GHz · Km su fibra monomodale, a seconda del laser utilizzato.

La terza finestra si colloca a 1550 nm, dove l'attenuazione è ancora inferiore e rappresenta una promessa per l'immediato futuro. Essa è presente solo nella fibra monomodale.

Le attenuazioni delle fibre ottiche variano in funzione del tipo di fibra e della finestra in cui lavorano:

- le fibre multimodali (50/125, 62.5/125), se lavorano in prima finestra hanno attenuazioni inferiori a 3.5 dB/Km, se lavorano in seconda finestra hanno attenuazioni inferiori a 1 dB/Km;
- le fibre monomodali, se lavorano in seconda finestra hanno attenuazioni inferiori a 0.5 dB/Km, se lavorano in terza finestra hanno attenuazioni inferiori a 0.2 dB/Km.

L'attenuazione introdotta da connettori e giunzioni deve essere paragonabile a quella molto bassa delle fibre ottiche: da 0.4 a 4 dB/Km. Un connettore installato correttamente introduce una attenuazione compresa tra 0.3 dB e 0.7 dB. Valori simili valgono per una giunzione (da 0.1 a 0.3 dB).

Le apparecchiature hanno un *optical power budget*, valore che indica l'attenuazione massima ammessa tra due apparati attivi, compreso tra 10 e 22 dB. Consentono normalmente di percorrere distanze di 1-2 Km con fibre multimodali e di 40-100 Km con fibre monomodali. Questo significa che nelle reti di telecomunicazioni le fibre ottiche devono avere ripetitori ogni 40-100 Km invece dei 2 Km tipici per i vecchi cavi coassiali in rame.

Come esempio di cavo in fibra ottica la figura 3.34 mostra in sezione il cavo bifibra AT&T 1861A.

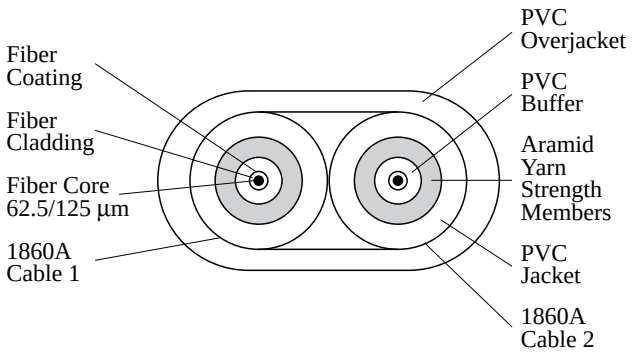


Fig. 3.34 - Cavo bifibra.

3.3.2 Caratteristiche costruttive dei cavi in fibra ottica

I cavi in fibra ottica vengono realizzati con tecniche diverse che variano in base al numero di fibre presenti ed al luogo in cui devono essere installati.

A seconda della metodologia costruttiva si identificano le tre principali famiglie di cavi in fibra ottica di seguito descritte.

I cavi di tipo *tight* sono usati principalmente per installazioni in luoghi interni; essi hanno le guaine protettive aderenti alla fibra e possono essere direttamente terminati con diversi tipi di connettori: ST, FC-PC, ecc. Si suddividono ulteriormente in due famiglie:

- i cavi *multimonofibra* (figura 3.35), indicati anche con i nomi *breakout* o *heavy duty*, sono particolarmente robusti in quanto il rivestimento sulla singola fibra può arrivare fino a 2 ÷ 3 mm di diametro;

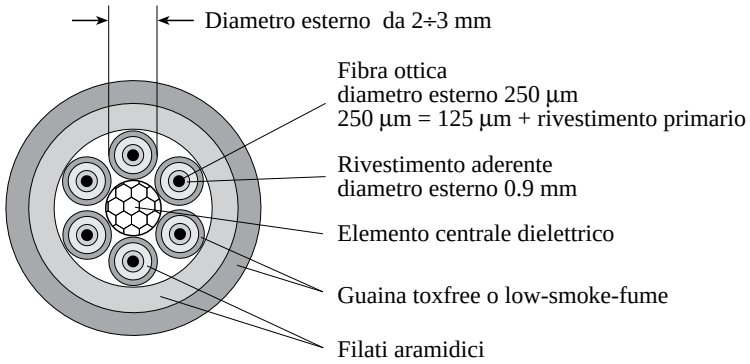


Fig. 3.35 - Cavo multimonofibra.

- i cavi *multifibra* (figura 3.36), indicati anche con i nomi: *light duty* o *trunk*, sono meno robusti dei precedenti poiché il rivestimento della singola fibra porta il diametro globale a 0.9 mm, ma sono piú adatti come cavi di dorsale poiché la ridotta dimensione di ogni singola fibra permette una maggiore densità di fibre ottiche.

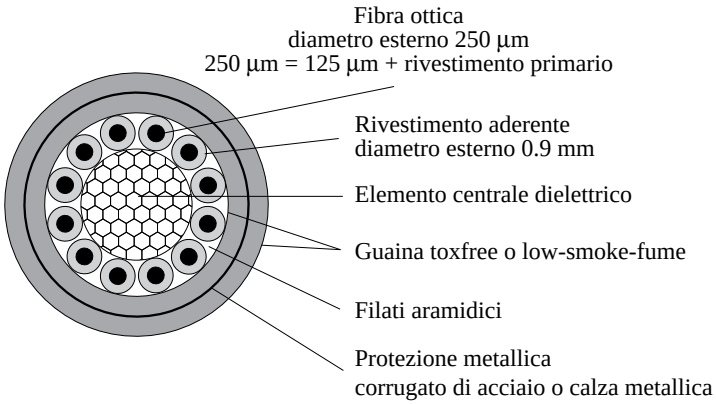


Fig. 3.36 - Cavo multifibra.

I cavi di tipo *loose* (figura 3.37) sono usati pricipalmente per installazioni in luoghi esterni; essi sono costituiti da un certo numero di tubetti, cordati attorno ad elemento centrale, entro cui vengono riposte le fibre nude (diametro 250 μm). Questi cavi non possono essere direttamente intestati sui connettori, ma devono essere giuntati, tramite tecniche di splicing o fusione, a cavetti monofibra di tipo tight. I cavi loose non sono molto facili da posare in modo verticale, perché la fibra all'interno della guaina si può disporre in modo anomalo. Inoltre, poiché la fibra ottica è molto sensibile all'umidità, si usano gel protettivi per tamponare il cavo.

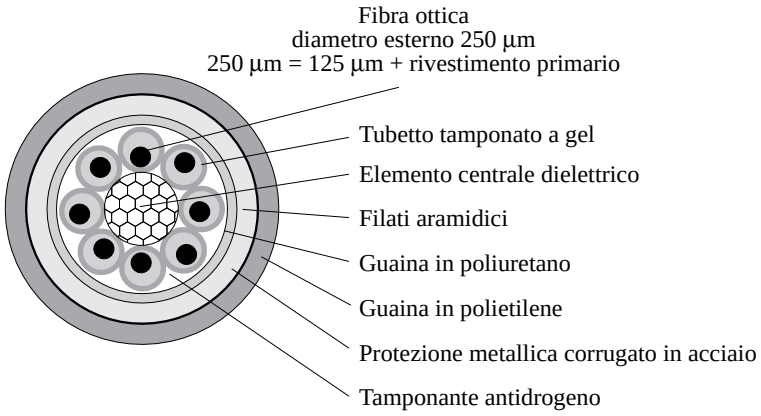


Fig. 3.37 - Cavo di tipo loose.

I *cavi di tipo "slotted core"* (figura 3.38) sono usati principalmente per installazioni in luoghi esterni; essi sono costituiti da un elemento centrale scanalato entro le cui cavità vengono riposte le fibre nude. Anche questi cavi non possono essere direttamente intestati sui connettori, ma devono essere giuntati, tramite tecniche di splicing o fusione, a cavetti monofibra di tipo tight.

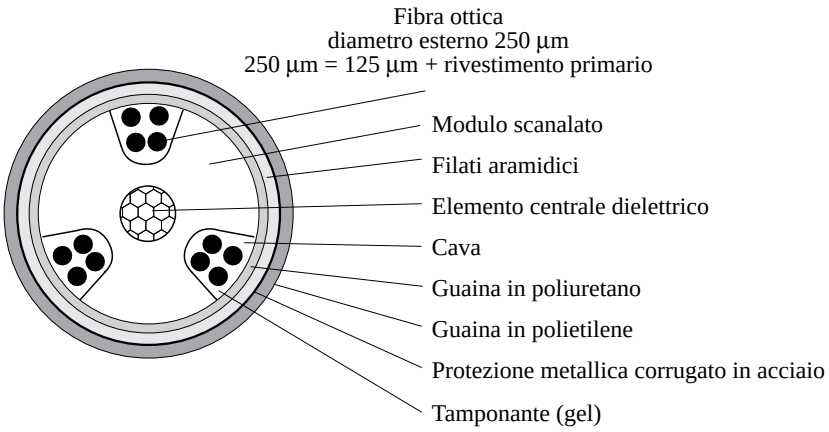


Fig. 3.38 - Cavo di tipo slotted core.

Il cavo è normalmente protetto da una corazza di acciaio corrugato termosaldato che può migliorare la robustezza meccanica e la resistenza all'acqua, e serve anche come protezione antiroditore.

3.4 MODALITA` DI UTILIZZO DEI CANALI TRASMISSIVI

I mezzi trasmissivi sino ad ora considerati possono essere impiegati in modo sia monodirezionale sia bidirezionale. La fibra ottica, per la sua struttura fisica, è un mezzo monodirezionale; il doppino viene normalmente impiegato come mezzo monodirezionale (anche se in telefonia lo si usa in modalità bidirezionale), mentre il cavo coassiale è normalmente utilizzato in modalità bidirezionale.

Nel caso di fibre ottiche e doppini, il collegamento tra due sistemi A e B è di tipo *punto-punto*, realizzato quindi con una coppia di fibre ottiche o con una coppia di doppini: uno per trasmettere da A verso B e l'altro per trasmettere da B verso A (figura 3.39).

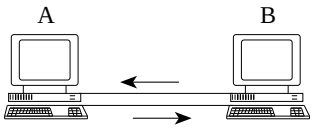


Fig. 3.39 - Canale punto-punto.

Questo canale trasmissivo prende anche il nome di canale punto-punto *full-duplex*, in quanto ammette contemporaneamente la trasmissione da A verso B e da B verso A.

Mentre le fibre ottiche permettono di realizzare solo canali trasmissivi punto-punto, con i doppini si possono realizzare sia canali punto-punto, sia canali punto-multipunto.

I canali *punto-multipunto* (detti anche *multidrop*, figura 3.40) sono dei canali half-duplex, in cui in un dato istante una sola stazione trasmette. Mentre A trasmette a B, B non può trasmettere e viceversa. Su tali canali si collegano un sistema master e più sistemi slave. Il sistema master decide chi deve trasmettere sul canale e i sistemi slave possono trasmettere solo su richiesta (*poll*) del sistema master. I canali punto-multipunto, ora in disuso, sono stati usati nel passato per interconnettere gruppi di terminali ad un elaboratore centrale.

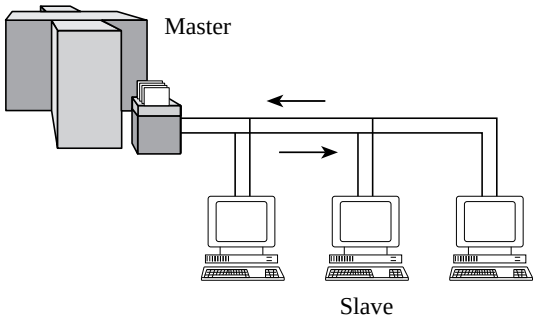


Fig. 3.40 - Canale punto-multipunto.

Con il cavo coassiale si possono realizzare sia canali punto-punto sia canali punto-multipunto, ma l'applicazione principale del cavo coassiale è la realizzazione di canali *broadcast* (figura 3.41) a cui sono collegati molti sistemi e in cui, quando un sistema trasmette, tutti gli altri ricevono. La trasmissione ad una determinata stazione avviene perciò sulla base di un indirizzo che deve essere incluso nel pacchetto di dati, e che la stazione destinataria riconosce.

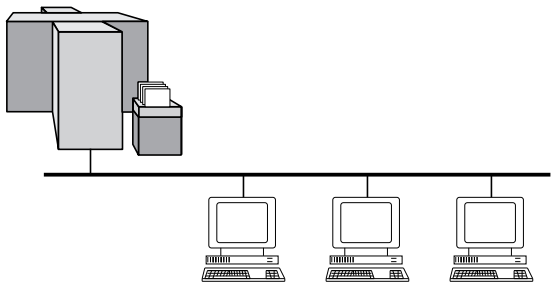


Fig. 3.41 - Canale broadcast.

3.5 TOPOLOGIE

Le topologie usate nelle reti di calcolatori sono molte e vanno dall'anello, alla stella, al bus, alla maglia completa o incompleta. Per le reti locali si adottano topologie semplici e regolari quali il bus, la stella o l'anello, mentre per le reti geografiche si adottano topologie parzialmente magliate. Le ragioni di scelte differenziate sono da ricercarsi nel diverso costo dei mezzi trasmissivi, basso nelle LAN e alto nelle WAN.

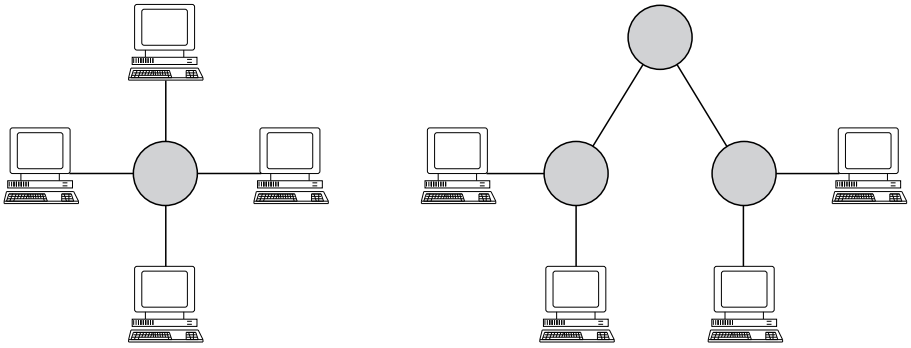
Topologie più o meno regolari implicano differenti problematiche di instradamento dei messaggi. Queste possono essere molto semplici, o addirittura non esistere, nelle topologie quali il bus o l'anello monodirezionale, ed essere anche molto complesse in reti magliate con topologie irregolari e canali a velocità differenziate.

3.5.1 La stella

La stella è una topologia interessante perché permette di precablare in modo strutturato gli edifici come spiegato nel capitolo 4. La topologia stellare (figura 3.42a) implica la presenza di un centro stella che può divenire un punto critico per l'affidabilità della rete, ma d'altro canto semplifica moltissimo la gestione e la manutenzione della rete stessa permettendo l'esclusione di sistemi malfunzionanti.

Molto spesso la stella è in realtà una stella gerarchica (a più livelli, come illustrato in figura 3.42b) e quindi, più propriamente, un albero.

Nelle stelle e negli alberi le problematiche di instradamento sono semplici poiché esiste un solo cammino che collega due sistemi.



(a) (b)

Fig. 3.42 - Topologie a stella.

La stella si realizza impiegando due mezzi trasmissivi punto-punto (normalmente doppino o fibra ottica) per interconnettere ogni sistema al centro stella (uno dal centro stella verso il sistema e l'altro in direzione opposta).

3.5.2 L'anello

La topologia ad anello prevede di collegare ogni sistema al sistema successivo con un mezzo trasmissivo punto-punto e di collegare l'ultimo sistema al primo (figura 3.43). Ne risulta un anello unidirezionale in cui ogni sistema ha anche una funzionalità di ripetizione dei messaggi degli altri sistemi. Infatti, quando un sistema deve trasmettere, esso inserisce il messaggio sull'anello trasmettendolo al sistema a valle. Tutti gli altri sistemi ripetono il messaggio sino a quando questo torna al sistema mittente che lo toglie dall'anello. Il sistema destinatario, oltre a ripetere il messaggio, lo riceve e può modificare un bit nella coda del messaggio per confermare l'avvenuta corretta ricezione al mittente. Questa caratteristica di "conferma dell'avvenuta ricezione" è peculiare solo delle reti ad anello.

La topologia ad anello unidirezionale è molto attrattiva da un punto di vista di organizzazione logica della rete, ma molto meno per quanto concerne il cablaggio fisico della rete stessa. Infatti, se una rete viene cablata ad anello, la sua affidabilità ne risulta gravemente compromessa: un sistema guasto o spento interrompe l'operatività dell'intera rete stessa. Per tale motivo per le reti ad anello si adottano cablaggi che consentano di escludere dalla rete sistemi o mezzi trasmissivi mal funzionanti.

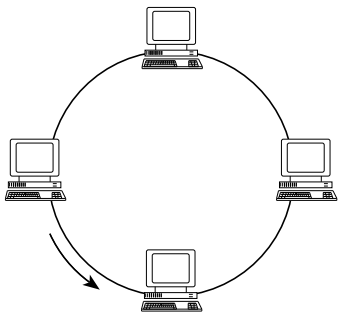


Fig. 3.43 - Topologia ad anello.

Si possono adottare due diverse soluzioni:

- scegliere un cablaggio a stella ripiegando l'anello sui centri stella (figura 3.44) ai quali affidare il compito di escludere i sistemi mal funzionanti tramite circuiti di "bypass" garantendo così l'affidabilità della rete;

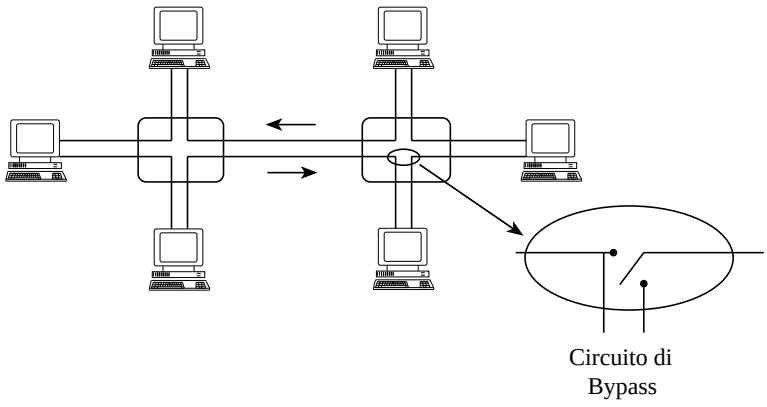


Fig. 3.44 - Rete ad anello cablata a stella.

- usare un cablaggio a doppio anello controrotante (figura 3.45), in cui si mantiene il cablaggio ad anello, ma si inserisce un secondo anello con funzionalità di backup in caso di guasto di un sistema. In questo secondo approccio il guasto contemporaneo di più sistemi porta al partizionamento dell'anello.

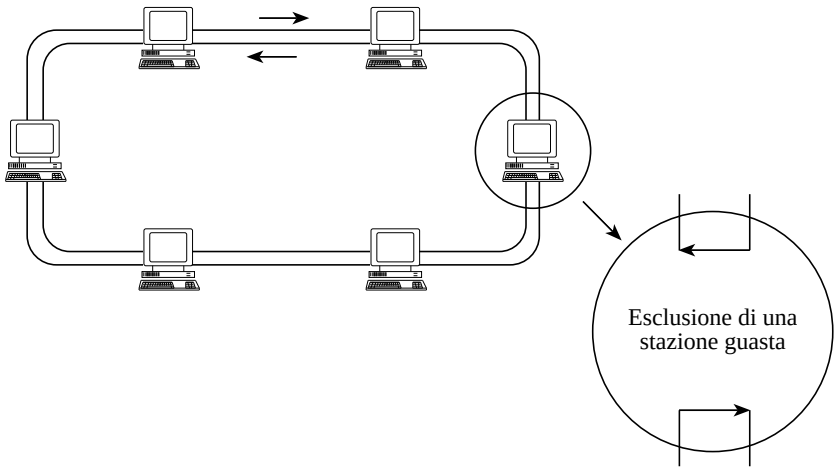


Fig. 3.45 - Rete ad anello cablata a doppio anello controrotante.

La seconda soluzione è tipicamente impiegata sulle dorsali, mentre la prima è più diffusa nell'interconnessione dei sistemi di utente.

3.5.3 Il bus

La topologia a bus (figura 3.46) richiede un mezzo trasmissivo intrinsecamente bidirezionale, cioè che ammetta la propagazione del segnale in entrambe le direzioni. Il bus è un mezzo trasmissivo broadcast in cui quando un sistema trasmette tutti gli altri ricevono simultaneamente. I sistemi collegati al bus non devono occuparsi di effettuare ripetizione o instradamento: tutti i sistemi sono raggiungibili direttamente. I bus si realizzano tipicamente con cavi coassiali.

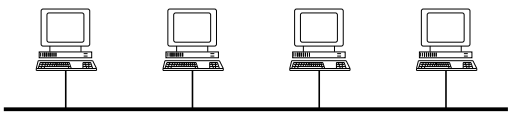


Fig. 3.46 - Topologia a bus.

Poiché il bus è un mezzo trasmissivo broadcast, esso è stato molto usato nelle LAN (in particolare in Ethernet) che, come spiegato nel capitolo 5, sono per loro natura broadcast. Inoltre, l'assenza di un elemento centrale, quale quello delle reti

a stella, garantisce una elevata affidabilità intrinseca.

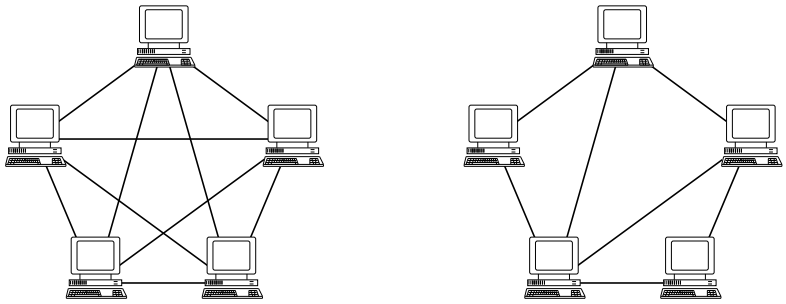
La topologia a bus mal si adatta al cablaggio strutturato che, come vedremo nel capitolo 4, impiega principalmente doppini e fibre ottiche con una topologia a stella gerarchica.

3.5.4 Le maglie

La topologia magliata prevede di interconnettere i sistemi con canali trasmissivi punto-punto bidirezionali, formando uno o più anelli. Se è prevista la connessione di ogni sistema con tutti gli altri si parla di maglia completa, in caso diverso di maglia incompleta.

La maglia completa (figura 3.47a) richiede un numero di canali trasmissivi che cresce in modo quadratico al crescere del numero dei sistemi. Per questo trova applicazione solo in reti molto piccole dove l'affidabilità sia un fattore determinante.

La maglia incompleta (figura 3.47b) trova invece la sua naturale applicazione nelle reti geografiche dove il fattore costo spingerebbe a configurare la rete ad albero per minimizzare il numero di canali trasmissivi. Essendo questi, su base geografica, meno affidabili di quelli su base locale, è necessario aggiungere alcuni canali ridondanti, magliando appunto la rete per aumentarne l'affidabilità.



(a) (b)

Fig. 3.47 - Topologie magliate.

Le topologie a maglia incompleta pongono problemi di instradamento e di bilanciamento del traffico sulle linee, essendo possibili in generale più cammini tra una coppia di sistemi.

BIBLIOGRAFIA

[1] BICC, "Cables for Structured Wiring Systems and Local Area Networks", Manuale BICC Cables Limited, Warrington (UK).

[2] Ceat Service, "Materiale illustrativo sui cavi", Ceat Service, Torino (Italia).

[3] Belden, "Networking Cables", Materiale illustrativo Belden Richmont (USA).

[4] Montorose, "Materiale illustrativo sui cavi", The Wire Group International, USA.

[5] EIA/TIA-568, "Commercial Building Telecommunication Wiring Standard", luglio 1991.

[6] EIA/TIA/TSB-36, "Technical Systems Bulletin Additional Cable Specification for Unshielded Twisted Pair Cables"; novembre 1991.

[7] EIA/TIA/TSB-40, "Additional Transmission Specifications for Unshielded Twisted-Pair Connecting Hardware", agosto 1992.

[8] ISO/IEC DIS 11801, "Information technology - Generic cabling for customer premises cabling", gennaio 1994.

[9] Optical Cable Corp. "Videocassetta su Fibre Ottiche", Roanoke, VA (USA).

[10] Videocassetta SSGRR, "Il Collaudo in opera dei cavi in fibra ottica", L'Aquila (Italia), gennaio 1989.

[11] Digital, "Guida alle reti Locali", 1982.

[12] IBMCentro di competenza Telecomunicazioni, "Reti Locali IBM: Sistema di cablaggio IBM", Codice documento GA13-1536-01, Roma (Italia), settembre 1989.

[13] AT&T Network System, "Systimax Premise Distribution System: Component Guide", Codice documento No. 555-400-603, dicembre 1990.

[14] J.E. McNamara, "Local Area Networks: an Introduction to the Technology".

[15] J.E. McNamara, "Technical Aspects of Data Communication", Digital Press, Bedford, MA (USA), 1988.

[16] U. Black, "Computer Networks: Protocols, Standard and Interfaces", Prentice Hall, Englewood Cliffs, N.J. (USA), 1987.

[17] Landee, Davis, Albrecht, Giacoletto, "Electronics designers' handbook", McGraw-Hill, New York (USA), 1977.

4

IL CABLAGGIO STRUTTURATO DEGLI EDIFICI

4.1 INTRODUZIONE

La trasmissione di segnali all'interno degli edifici riveste oggi un'importanza tale da richiedere la presenza di infrastrutture permanenti al pari di quelle idrauliche o di alimentazione elettrica. La costruzione o la ristrutturazione di un edificio è un'occasione preziosa per predisporre un impianto tecnologico per la trasmissione dell'informazione in tutte le sue varie forme (figura 4.1): reti locali, immagini video, telefonia, allarmi, ecc. Tale impianto tecnologico prende il nome di *sistema di cablaggio*. Questo capitolo affronta il problema della progettazione razionale di sistemi di cablaggio multifunzionali (sistemi di cablaggio *strutturato*), analizzando sia gli standard internazionali, sia i principali prodotti disponibili sul mercato.

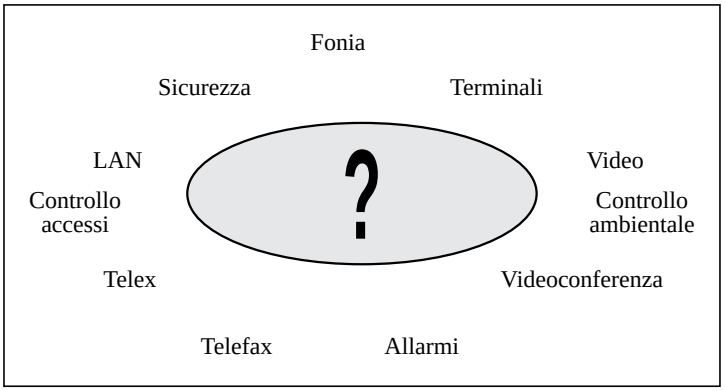


Fig. 4.1 - Cosa integrare.

Le normative sui sistemi di cablaggio definiscono metodi per cablare un gruppo di edifici costruiti su un comprensorio (campus), cioè su un singolo appezzamento di suolo privato o su un insieme di appezzamenti vicini collegati da opere edilizie permanenti (sovrappassi o sottopassi).

Le normative descrivono:

- le caratteristiche dei mezzi trasmissivi e dei componenti passivi (connettori, permutatori, giunti meccanici, terminatori, prese utente, adattatori, ecc.), in relazione alle velocità trasmissive desiderate;
- le topologie di cablaggio ammesse (stella, anello, bus, maglia) e le caratteristiche ad esse riferite quali, ad esempio, eventuali livelli di gerarchia, distanze massime, adattamenti tra diverse topologie;
- le regole di installazione e le indicazioni sulla documentazione di progetto.

L'esigenza di disporre di sistemi di cablaggio per i sistemi informativi è nata all'inizio degli anni '80 in seguito alla sempre maggiore necessità di connettere apparecchiature elettroniche, in particolare terminali sincroni e asincroni. In quegli anni sono nate anche le prime reti locali Ethernet e Token Ring e di conseguenza si sono sviluppati anche i primi sistemi di cablaggio proprietari, ad esempio IBM cabling system e Digital DECconnect.

Verso la fine degli anni '80 si è assistito ad un'evoluzione delle reti locali, che abbandonarono i mezzi trasmissivi proprietari e iniziarono ad utilizzare in modo sistematico il doppino di rame 24 AWG e la topologia a stella. Questa scelta aveva come obiettivo creare una sinergia con i sistemi di cablaggio per telefonia e nacquero i primi cablaggi "fonia-dati".

Da quel momento l'evoluzione è stata incessante e sorse presto il problema di emettere normative di riferimento per i sistemi di cablaggio. Il primo standard è nato da una proposta congiunta di due comitati americani: l'EIA (associazione delle industrie elettroniche) e la TIA (associazione delle industrie di telecomunicazioni). Essi proposero uno standard per il cablaggio degli edifici commerciali denominato *EIA/TIA 568*. La maggior parte dei costruttori adeguò ad esso i propri prodotti, e, nel luglio 1991, l'ANSI lo ratificò per gli USA.

Per alcuni anni l'EIA/TIA 568 è stato il riferimento anche al di fuori degli Stati Uniti, ma nel 1994 è stata approvata una proposta di standard internazionale che rappresenta l'evoluzione dello standard americano: l'ISO/IEC 11801.

È evidente che, per garantire la massima versatilità, i sistemi di cablaggio devono essere progettati pensando agli utilizzi che necessitano della maggior banda trasmissiva. Per questo motivo vi è un forte legame tra l'architettura dei sistemi di cablaggio e quella delle reti locali, le cui specifiche sono le più stringenti tra gli attuali servizi di trasmissione dei segnali.

4.2 SISTEMI DI CABLAGGIO PROPRIETARI

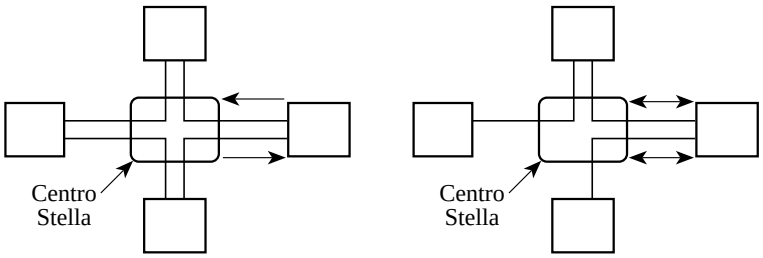
Negli anni '80 si sono resi disponibili sul mercato diversi sistemi di cablaggio, tra i quali due hanno avuto successo: il Cabling System IBM ed il DECconnect Digital.

4.2.1 Cabling System IBM

L'obiettivo è di unificare i precedenti cablaggi IBM con un unico sistema di cablaggio in grado di interconnettere terminali e stampanti ed essere un valido supporto fisico per le reti Token Ring.

La topologia di questo sistema di cablaggio è di tipo stellare e permette l'interconnessione anche di apparati concepiti per tipi di distribuzione diversi quali il bus o l'anello. In questi casi si opera sull'armadio di distribuzione e, tramite l'uso di cavi di adattamento, si costruisce una topologia logica a bus o ad anello, sfruttando il cablaggio a stella, in modo analogo a quanto illustrato in figura 4.2. Il cavi utilizzati per il cablaggio sono di due tipi (si veda il paragrafo 3.2.8):

- il tipo 1 IBM, per trasmissione dati;
- il tipo 2 IBM, per fonia e dati.



(a) Anello cablato a stella (b) Bus cablato a stella

Fig. 4.2 - Flessibilità del cablaggio a stella.

Sui pannelli di permutazione e sulle placchette utente viene utilizzato un particolare connettore detto "ermafrodita" perché è allo stesso tempo maschio e femmina: infatti è possibile giuntare direttamente due di questi connettori ruotandoli di 180 gradi. La figura 4.3 mostra l'aspetto del connettore ermafrodita.

Gli apparati IBM, a seconda dei modelli, possono utilizzare diversi tipi di cavi: STP, coassiali, biassiali, i quali possono anche avere impedenze diverse. Per adattare le impedenze richieste dalle diverse apparecchiature a quella del cavo di

tipo 1, vengono utilizzati una serie di cavi di adattamento, eventualmente contenenti un balun (si veda il paragrafo 3.2.7), ed aventi da un lato il connettore ermafrodita e dell'altro l'opportuno connettore per il collegamento all'apparecchiatura. In figura 4.4 è schematizzato un cavo di adattamento per apparati di tipo 3270.

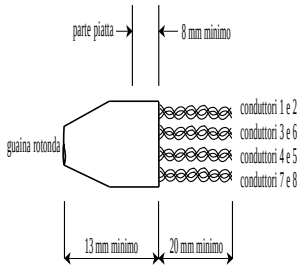


Fig. 4.3 - Connettore ermafrodita.

Fig. 4.4 - Cavo di adattamento per terminale IBM 3270.

Nella figura 4.5 è riportato un esempio di cablaggio in cui si vedono le connessioni tra l'armadio di distribuzione, un terminale ed un personal computer.

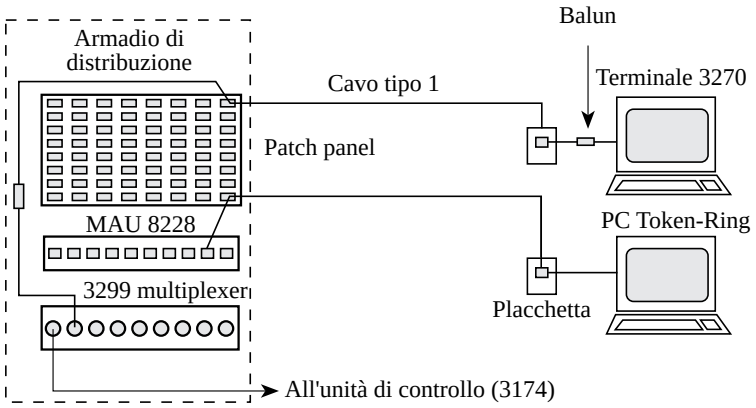


Fig. 4.5 - Esempio di cablaggio IBM.

4.2.2 DECconnect Digital

L'obiettivo è quello di avere un sistema di cablaggio adatto ad interconnettere terminali e stampanti di tipo asincrono e offrire un supporto per le reti Ethernet.

La topologia è di tipo stellare per ciò che riguarda i collegamenti seriali asincroni e di tipo a bus per i collegamenti Ethernet.

I cavi utilizzati per il cablaggio sono di due tipi:

- cavo UTP a 3 coppie per i collegamenti seriali;
- cavo thin Ethernet per la rete locale.

Per la presa di utente e per gli armadi di permutazione si utilizzano i seguenti connettori:

- DEC423 (connettore a 6 contatti con chiave spostata) per le connessioni seriali asincrone;
- BNC per Ethernet.

Nella figura 4.6 è riportato un esempio in cui si vedono le connessioni tra l'armadio di distribuzione e il terminale o i PC.

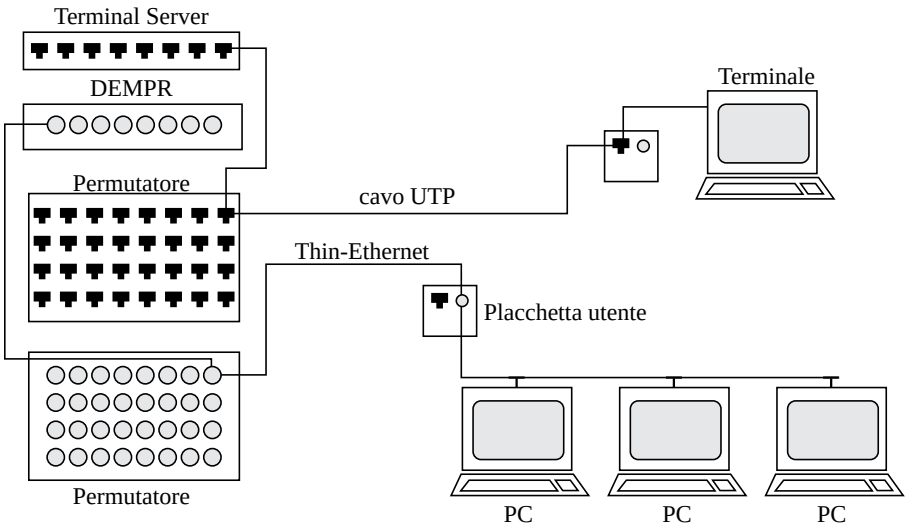


Fig. 4.6 - Esempio di cablaggio DECconnect.

4.3 GLI STANDARD INTERNAZIONALI

Esistono oggi i seguenti standard per i sistemi di cablaggio:

- *EIA/TIA 568:* è uno standard americano per il cablaggio di edifici commerciali; è stato approvato nel luglio 1991 ed è attualmente quello più applicato e diffuso in tutto il mondo;
- *EIA/TIA 570:* è uno standard americano per il cablaggio di edifici residenziali, occupati da una singola famiglia o più occupanti, che possono avere un numero ridotto di uffici commerciali. In questo caso è preponderante l'aspetto della distribuzione delle linee telefoniche esterne;
- *ISO/IEC DIS 11801* è una proposta di standard internazionale per i cablaggi di edifici commerciali che è stata votata ed approvata nel luglio 1994. I paesi europei sono particolarmente interessati a questa normativa che viene sempre più richiesta come requisito base per la realizzazione di cablaggi strutturati;
- *SP-2840-A* è una proposta di revisione dello standard EIA/TIA 568 per far fronte alle esigenze di maggiori velocità trasmissive sui cablaggi; dovrebbe essere approvata nel luglio 1995 e prenderà il nome EIA/TIA-568-A;
- *prEN 50173* è una proposta di standard europeo che non è ancora stata approvata ed è molto simile ad ISO/IEC DIS 11801.

I cablaggi devono essere certificati con appositi strumenti di misura per garantire determinate prestazioni, e il gruppo di lavoro TR41.8.1 del comitato EIA/TIA ha preparato una bozza di normativa americana che a seguito dell'approvazione prenderà il nome di bollettino *TSB67*.

Inoltre, per poter realizzare correttamente un sistema di cablaggio è necessario che tutte le infrastrutture di tipo meccanico ed edile rispondano a determinati requisiti. Questi aspetti sono trattati dallo standard americano *EIA/TIA 569*.

Infine, lo standard *TIA/EIA 607* tratta il problema della realizzazione di un impianto di messa a terra adeguato ad un cablaggio strutturato.

4.4 LO STANDARD EIA/TIA 568

Questo standard specifica i requisiti minimi richiesti per il cablaggio di un edificio o un gruppo di edifici facenti parte di uno stesso comprensorio (figura 4.7).

I limiti del comprensorio sono i seguenti:

- l'estensione geografica massima è di 3.000 m;
- la superficie massima degli edifici è di 1.000.000 m^2;
- la popolazione massima degli edifici è di 50.000 persone.

La validità minima di un progetto è di dieci anni, e ciò significa che durante questo intervallo di tempo non deve essere necessario apportare al cablaggio modifiche sostanziali. Esso inoltre deve fornire un supporto adatto a diversi apparati di telecomunicazione e quindi deve essere indipendente da essi.

Lo standard prevede che il cablaggio venga realizzato contestualmente alla costruzione o ristrutturazione organica di un edificio, ma va osservato che è spesso applicato anche ad installazioni in edifici che non si trovano in tali condizioni, ma semplicemente in fase di rinnovamento della rete locale. In tali circostanze gli unici servizi che interessano sono normalmente la telefonia e la trasmissione dati.

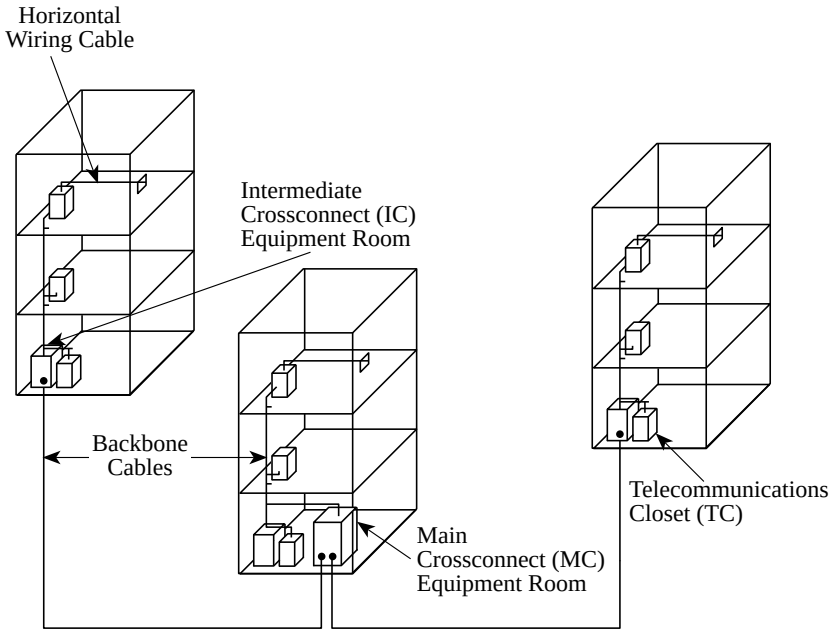


Fig. 4.7 - Modello EIA/TIA 568.

Le specifiche dello standard riguardano:

- la topologia;
- gli elementi facenti parte del cablaggio;

- i mezzi trasmissivi;
- le dorsali;
- il cablaggio orizzontale;
- le norme d'installazione;
- l'identificazione dei cavi;
- la documentazione.

4.4.1 La topologia

La topologia del cablaggio è di tipo *stellare gerarchica* (figura 4.8) e di conseguenza le altre topologie, ad esempio quella a bus e quella ad anello, tipiche di alcuni standard per LAN, devono essere ricondotte ad una topologia stellare.

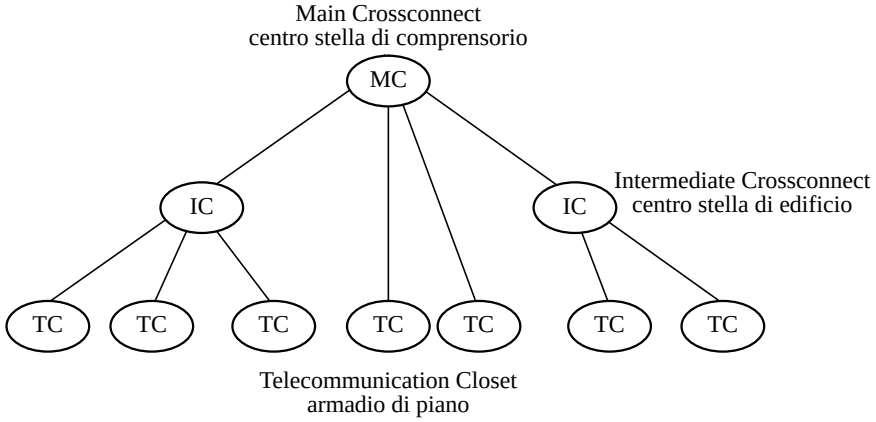


Fig. 4.8 - Topologia a stella gerarchica.

4.4.2 Elementi del cablaggio

Gli elementi costituenti un sistema di cablaggio sono: il main crossconnect, gli intermediate crossconnect, i telecommunication closet, l'interbuilding backbone, l'intrabuilding backbone, i transition point, i patch panel, i wiring block, i cross-connect, i telecommunication outlet e gli adapter. Ad essi si aggiungono alcuni elementi citati dallo standard, ma non soggetti a specifiche, quali la work area, l'equipment room, l'interbuilding entrance facility e il private branch exchange.

Il *Main Crossconnect* (MC), permutatore principale, identifica un locale tecnologico od un armadio di distribuzione, situato nell'edificio centrale o principale di un comprensorio, da cui vengono distribuiti i cavi di dorsale agli altri edifici. Esso è il primo livello di gerarchia del cablaggio (centro stella di comprensorio o di un edificio singolo). La figura 4.9 mostra un esempio di main crossconnect, collocato all'interno di una Equipment Room.

L'*Intermediate Crossconnect* (IC), permutatore intermedio, identifica il locale tecnologico o l'armadio di distribuzione di un edificio facente parte di un comprensorio, da cui vengono distribuiti i cavi di dorsale di edificio ai vari piani. Esso è il secondo livello di gerarchia del cablaggio (centro stella di edificio).

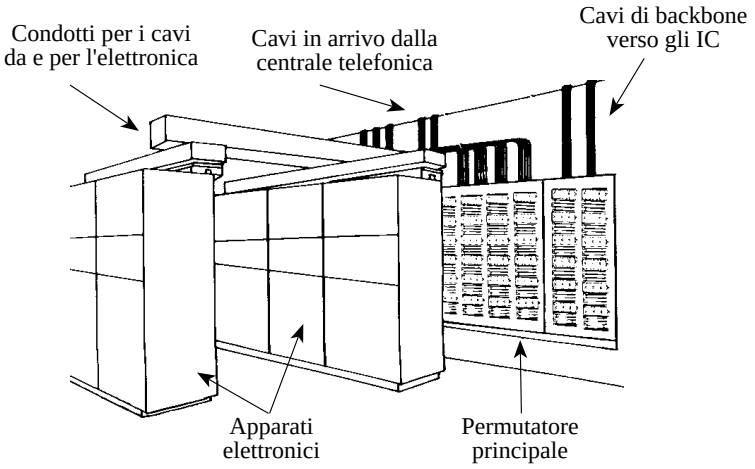


Fig. 4.9 - Esempio di Main Crossconnect all'interno di una Equipment Room.

Quando si realizza un cablaggio su un singolo edificio, il locale tecnologico o l'armadio di distribuzione di edificio diventa il primo livello gerarchico e quindi viene considerato Main Crossconnect.

Il *Telecommunication Closet* (TC) identifica l'armadio di piano da cui vengono distribuiti i cavi che raggiungono l'utenza. Esso è il terzo livello di gerarchia del cablaggio (centro stella di piano). La figura 4.10 mostra un esempio di armadio di piano.

L'*interbuilding backbone* (dorsale di comprensorio) è la dorsale di interconnessione tra l'edificio centro stella di comprensorio ed un altro edificio. Essa parte dal Main Crossconnect e termina su un Intermediate Crossconnect.

L'*intrabuilding backbone* (dorsale di edificio) è la dorsale di interconnessione tra il locale tecnologico di edificio e l'armadio di piano.

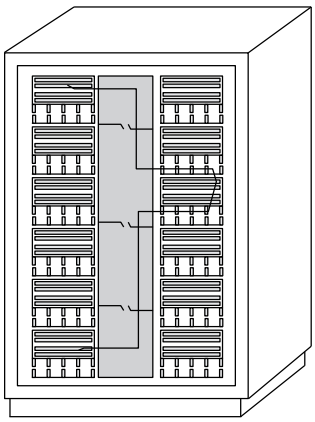


Fig. 4.10 - Esempio di armadio di piano.

L'*Equipment Room* (ER) è un locale tecnologico che può contenere degli apparati passivi, quali pannelli di permutazione, scaricatori di tensione, canaline e passacavi, e può ospitare apparati attivi quali il centralino telefonico, i concentratori per reti locali e le apparecchiature audio e video (figura 4.9). Il locale tecnologico ha una funzione molto simile ad un gruppo di armadi di distribuzione, ma le maggiori dimensioni a disposizione lo rendono più adatto al compito di centro stella di comprensorio o di edificio.

L'*interbuilding Entrance Facility* (EF) identifica un insieme di infrastrutture e di componenti passivi utilizzati per l'ingresso delle dorsali di comprensorio nell'edificio. Nell'EF è richiesto l'utilizzo di protezioni elettriche per i cavi in rame e deve essere particolarmente curato l'aspetto della messa a terra dei vari componenti.

Il *Transition Point* (TP) è un punto di transizione del cablaggio orizzontale dove un cavetto rotondo di tipo ritorto (twisted) viene connesso, tramite un giunto meccanico, ad un cavo piatto che è normalmente pre-intestato. È bene ricordare che questa possibilità va usata solo per trasmissione a basse frequenze (decine di KHz) in quanto il cavetto piatto ha pessimi valori di diafonia poiché le coppie non sono ritorte.

La *Work Area* (WA) identifica il posto di lavoro o la scrivania dell'utente.

Il *Private Branch eXchange* (PBX) è il centralino telefonico.

Il *patch panel* è un pannello di permutazione per i mezzi trasmissivi che può assumere due forme:

- per cavi in rame, può contenere uno o più blocchi di terminazione;
- per fibre ottiche, può contenere una serie di connettori passanti, chiamati barrel o bussole, che servono a permutare le fibre tra pannelli diversi oppure tra un pannello ed un apparato attivo.

Il *patch cord* è un cavetto di permutazione per cavi in rame o per fibre ottiche. Quando è per le fibre ottiche assume anche il nome di bretella ottica.

La terminazione meccanica dei cavi in rame viene fatta su blocchi di terminazione chiamati anche *wiring block*. La terminazione dei cavi in fibra ottica viene effettuata su appositi pannelli.

Un *cross-connect* (permutatore) è composto da almeno due blocchi di terminazione, di cui uno per i cavi entranti ed uno per i cavi uscenti. La figura 4.11 mostra un esempio di permutatore.

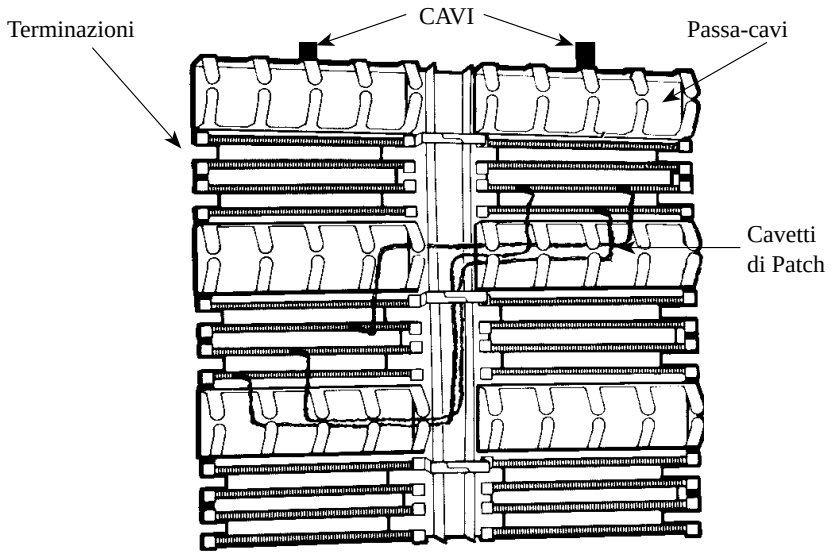


Fig. 4.11 - Permutatore AT&T PDS.

Il *Telecommunication Outlet* (TO) è la presa utente che può contenere due o più connettori (figura 4.12).

L'*adapter* è un adattatore per il cablaggio, e lo standard prevede che sia installato esternamente alle prese utente. Esso può essere:

- di tipo passivo, per adattare tipologie diverse di connettori o cavi; esempi di adapter sono i cavi adattatori, i balun, i media filter e i connettori ad "Y" (figura 4.13);
- di tipo attivo, per adattare sistemi trasmissivi diversi, ad esempio convertitori RS232-RS423, minimodem, ecc.

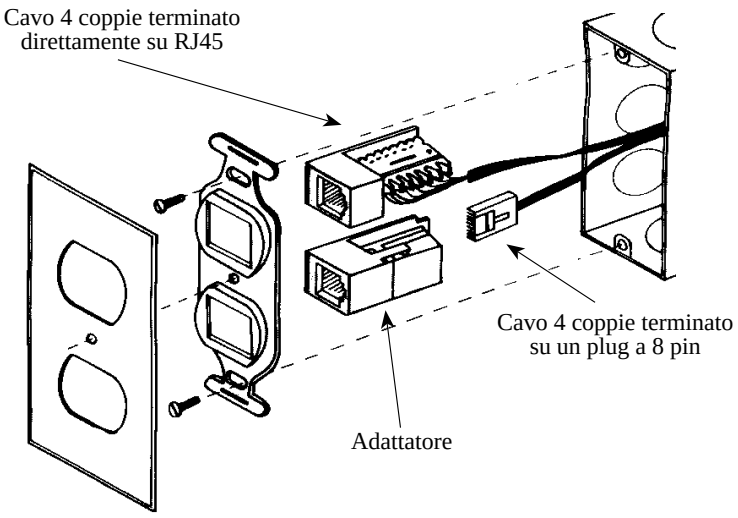


Fig. 4.12 - Presa a muro AT&T PDS.

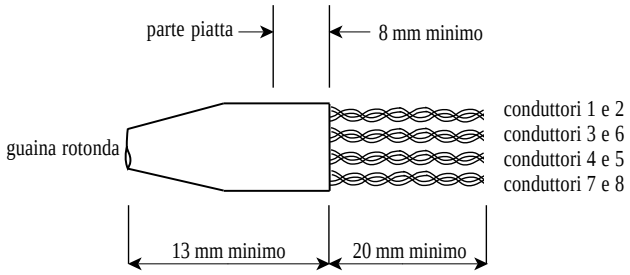


Fig. 4.13 - Adattatore a "Y".

4.4.3 I mezzi trasmissivi

I mezzi trasmissivi ammessi sono i seguenti:

- cavi coassiali da 50 Ω;
- fibre ottiche multimodali 62.5/125 μm;
- cavi UTP a 4 coppie;
- cavi UTP multicoppia;
- cavi STP a 150 Ω.

Le caratteristiche richieste per cavi coassiali sono quelle specificate dagli standard IEEE 802.3, 10Base5 e 10Base2 (si vedano i paragrafi 6.4.8 e 6.4.10).

La fibra ottica multimodale ammessa è quella di dimensioni 62.5/125 μm; le caratteristiche ottiche richieste sono quelle indicate nella tabella 4.1.

Lunghezza d'onda (nm)	Attenuazione massima (dB/Km)	Banda passante (MHz · Km)
850	3.75	160
1300	1.5	500

Tab. 4.1 - Caratteristiche della fibra ottica 62.5/125 μm.

I cavi UTP a 4 coppie hanno la dimensione di ogni singolo conduttore pari a 24 AWG. Essi devono soddisfare almeno le caratteristiche di categoria 3 (le categorie dei cavi UTP sono riportate nelle tabelle 3.4 e 3.5). Le coppie vengono identificate con i seguenti colori:

- coppia 1: bianco-blu (W-BL) e blu (BL);
- coppia 2: bianco-arancio (W-O) e arancio (O);
- coppia 3: bianco-verde (W-G) e verde (G);
- coppia 4: bianco-marrone (W-BR) e marrone (BR).

Il diametro esterno del cavo (guaina compresa) non deve superare la dimensione di 6.35 mm.

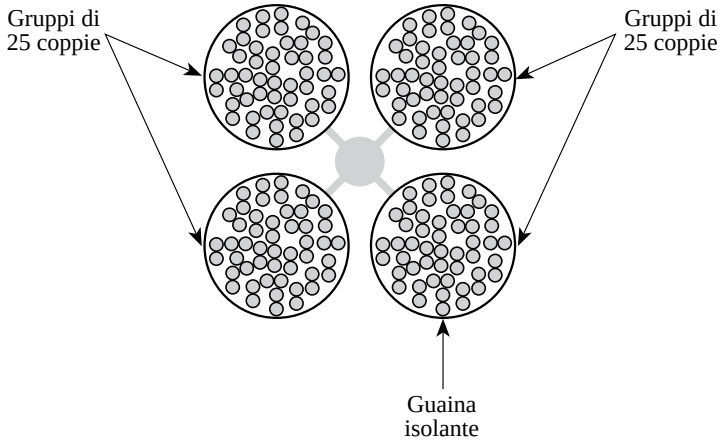


Fig. 4.14 - Cavo a 100 coppie.

I cavi UTP multicoppia contengono uno o più gruppi da 25 coppie cadauno (figura 4.14), i conduttori hanno una dimensione di 24 AWG, ma vengono accettati anche conduttori da 22 AWG, purché siano rispettate le caratteristiche elettriche minime richieste. Ogni singolo gruppo da 25 coppie ha una propria guaina isolante. Le caratteristiche elettriche minime dei cavi multicoppia sono riportate nelle tabelle 4.2 e 4.3.

Le caratteristiche dei cavi STP a 150 Ω sono quelle del cavo di "tipo 1" IBM (si veda il paragrafo 3.2.8).

Caratteristiche del cavo			Cavo a 25 coppie
Caratteristiche elettriche @ 20 °C	Unità di misura	MHz	
Near End Crosstalk (NEXT), minimo valore ammesso	dB @ 100 m	0.150	52
		0.772	41
		1.576	37
		3.15	32
		6.3	28
		10	25

Tab. 4.2 - Cavi a 25 coppie - diafonia.

Caratteristiche del cavo			Cavo a 25 coppie
Caratteristiche elettriche @ 20 °C	Unità di misura	MHz	
Impedenza	Ω	1÷16	100 +/- 15%
Mutua capacità di ogni coppia	nf/100 m	0.001	6.25
Minima velocità di propagazione			0.6 c
Massimo valore di resistenza	Ω/100 m		9.4
Attenuazione massima ammessa	dB/100 m	0.064	0.92
		0.256	1.31
		0.512	1.84
		0.772	2.2
		1	2.5
		4	5.06
		8	7.33
		10	8.22
		16	10.52

Tab. 4.3 - Cavi a 25 coppie - caratteristiche elettriche.

4.4.4 Le dorsali

Le dorsali sono gli elementi portanti del cablaggio e possono interconnettere, con topologia stellare gerarchica (figura 4.15):

- edifici diversi con l'edificio centro-stella del comprensorio (interbuilding backbone);
- armadi di piano diversi con l'armadio di edificio (intrabuilding backbone).

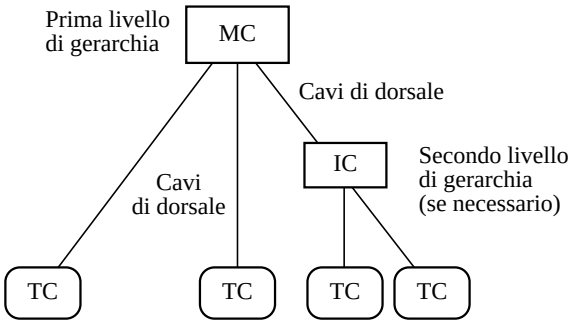


Fig. 4.15 - Architettura stellare gerarchica delle dorsali.

Le distanze massime ammesse per le dorsali variano a seconda dei mezzi trasmissivi utilizzati e di ciò che essi interconnettono; la figura 4.16 mostra i limiti massimi di lunghezza delle dorsali.

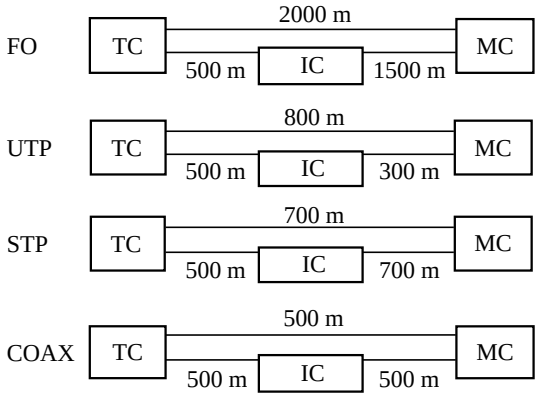


Fig. 4.16 - Distanze massime ammesse sulle dorsali.

I cavi ammessi sono i seguenti:

- fibra ottica multimodale 62.5/125μm;
- cavo multicoppia a 100 Ω;
- cavo STP a 150 Ω;
- cavo coassiale a 50 Ω, tipo thick Ethernet, intestato alle due estremità con appositi connettori detti di tipo "N".

Quando si utilizzano dei cavi di rame bisogna considerare la possibilità di introduzione o emissione di disturbi elettromagnetici. In caso di ambienti caratterizzati da forte rumore elettromagnetico o dove, per la sensibilità delle apparecchiature ivi contenute, i cavi di dorsali possano essere fonte di disturbo, è consigliabile utilizzare le fibre ottiche.

4.4.5 Il cablaggio orizzontale

Il cablaggio orizzontale interconnette i vari posti di lavoro all'armadio di piano e deve essere progettato per fornire almeno i seguenti servizi:

- trasporto di fonia;
- trasmissione dati in modalità seriale;
- trasporto dati per le reti locali;
- trasporto di segnali per il controllo di dispositivi all'interno dell'edificio (ad esempio termostati).

La topologia è di tipo stellare a partire dall'armadio di piano. Le distanze massime ammesse per i cavi di distribuzione ed i cavetti di permutazione sono indicate nella figura 4.17.

I cavi ammessi sono i seguenti:

- cavo UTP a 4 coppie con impedenza da 100 Ω;
- cavo STP a 2 coppie con impedenza da 150 Ω;
- cavo coassiale da 50 Ω, tipo Ethernet sottile (thin), intestato alle due estremità con appositi connettori detti BNC;
- fibra ottica multimodale 62.5/125 μm.

La placchetta o presa a muro, relativa al singolo posto di lavoro, deve contenere almeno due cavi, di cui almeno uno deve essere di tipo UTP a 4 coppie di categoria 3 o superiore. Il cavo UTP va intestato su una presa RJ45 (figura 4.18). Il secondo cavo può essere uno qualunque dei cavi ammessi per il cablaggio

orizzontale sopra elencati, compreso un secondo cavo UTP, che è attualmente la soluzione più adottata.

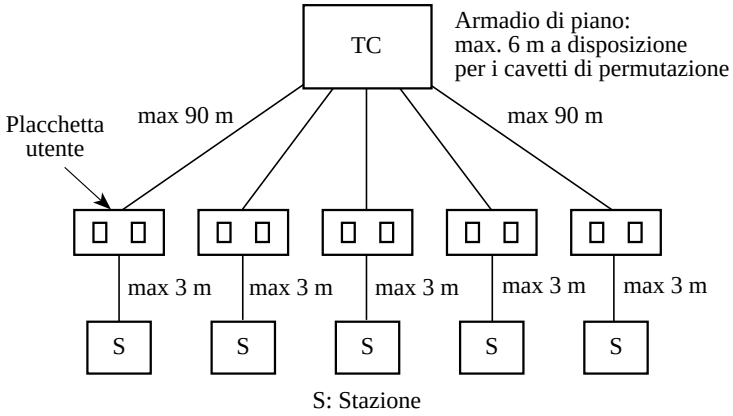
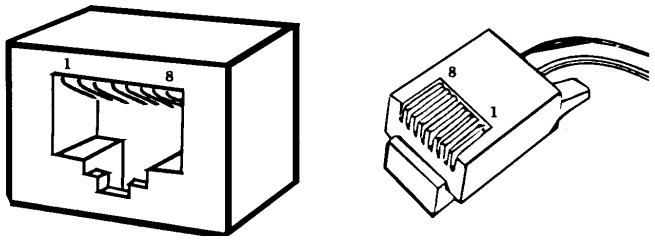


Fig. 4.17 - Distanze massime ammesse sul cablaggio orizzontale.

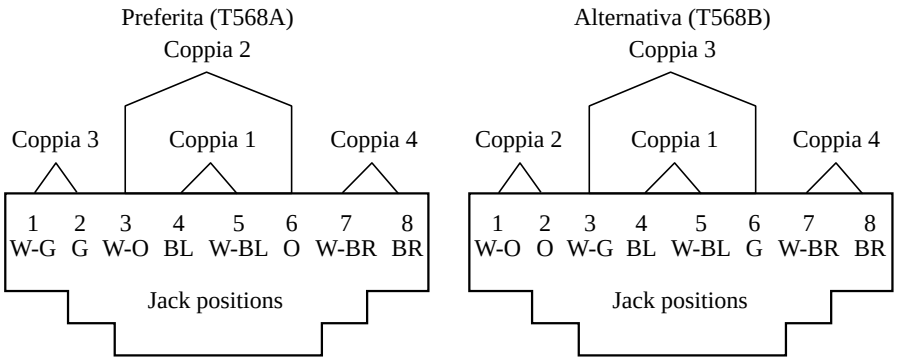


Presa femmina da parete Spinotto (plug) maschio volante

Fig. 4.18 - RJ45: connettore a 8 contatti con chiave centrale.

Il cavo UTP può essere intestato sulla presa RJ45 in due differenti modi: uno "preferito" ed un secondo "alternativo", quest'ultimo utilizzato nei cablaggi PDS AT&T. La figura 4.19 mostra la diversa assegnazione delle coppie.

È possibile derivare due servizi dalla medesima presa utente tramite l'utilizzo di un derivatore ad "Y", illustrato nella figura 4.13.



Vista frontale del connettore RJ45

Fig. 4.19 - Assegnazione delle coppie.

4.4.6 Le norme d'installazione

Lo scopo di questo standard non è di fornire tutte le norme d'installazione, ma di considerare almeno gli aspetti più importanti che hanno un notevole impatto sulla qualità del cablaggio. Questi aspetti riguardano l'installazione dei cavi, il cablaggio sotto moquette e la messa a terra.

Il cablaggio, a seconda dei componenti utilizzati e della qualità dell'installazione, potrà essere considerato di categoria 3, 4 o 5. Un cablaggio di una determinata categoria deve avere come minimo tutti i componenti con le caratteristiche di tale categoria o superiore. Ad installazione avvenuta è necessario certificare, con appositi strumenti, l'intero cablaggio per verificarne la reale rispondenza alle specifiche.

Norme per l'installazione dei cavi UTP:

- la massima tensione di tiro applicabile sui cavi è di 11.3 Kg. Se si supera questo valore viene compromessa la corretta geometria delle coppie e si ha un conseguente degrado delle caratteristiche elettriche;
- il raggio di curvatura minimo ammesso varia a seconda della categoria del cablaggio. Il valore richiesto è di 25.4 mm per i cablaggi di categoria 3, ed otto volte il diametro esterno del cavo (50.8 mm) per i cablaggi di categoria 4 e 5;
- la parte del cavo non ritorta sulla terminazione non deve superare i 25 mm per i cablaggi di categoria 4, e 13 mm per i cablaggi di categoria 5.

Norme per il cablaggio sotto-moquette (under-carpet):

- il cablaggio non deve essere effettuato in locali umidi o soggetti al rovesciamento di solventi;
- si raccomanda che la pavimentazione sia realizzata con dei moduli quadrati per facilitare l'accesso al cablaggio;
- i cavi di telecomunicazione di tipo under-carpet possono incrociare i cavi di potenza a patto che questi non siano del tipo under-carpet;
- la distanza minima tra i cavi di telecomunicazione e quelli di potenza, quando viaggiano paralleli tra di loro, è di 152 mm.

La messa a terra va effettuata sui seguenti tipi di cavi:

- cavi di tipo schermato;
- cavi in fibra ottica ove sia presente una protezione meccanica di tipo metallico.

Le regole da rispettare sono quelle vigenti nella nazione in cui viene realizzato il cablaggio o quelle del costruttore di apparecchiature, nel caso in cui siano più restrittive delle precedenti.

4.4.7 Identificazione dei cavi

Per facilitare il compito di chi deve gestire ed effettuare la manutenzione dei sistemi di cablaggio, che potrebbero anche risiedere in edifici diversi ed essere stati realizzati da aziende diverse, è necessario unificare le metodologie di identificazione dei cavi.

Lo standard specifica che i cavi di dorsale devono avere un numero unico che deve contenere almeno due campi indicanti:

- l'identificativo del cavo;
- il numero di coppie, nel caso di cavo multicoppie, o il numero di fibre nel caso di cavo multifibra.

Un esempio di numerazione di un cavo di dorsale è il seguente: *"4005/1-300"*, che indica un cavo con il numero 4005 e contenente le coppie da 1 a 300.

Ogni posto di lavoro ed il relativo cavo sono identificati con una targhetta, composta normalmente da 8-10 caratteri, che può contenere numeri o lettere alfabetiche. La numerazione deve contenere:

- il riferimento al piano dell'edificio dove è situato il posto di lavoro;

- il riferimento all'armadio di piano a cui il posto di lavoro è stato collegato;
- un campo di tre caratteri che identifica il posto di lavoro stesso.

Normalmente gli armadi di piano vengono identificati con delle lettere alfabetiche.

Un esempio di come si numera il posto di lavoro ed il relativo cavo è rappresentato dalla targhetta: *"PG04102F"* il cui significato è il seguente:

- PG indica il nome dell'edificio che è: "Palazzo Galileo";
- 04 indica il piano in cui è situato il posto di lavoro;
- 102 è l'identificativo del posto di lavoro;
- F è l'identificativo dell'armadio di piano a cui il posto di lavoro è stato collegato.

4.4.8 Documentazione

Per ogni cablaggio bisogna fornire una documentazione redatta con simbologia e abbreviazioni standard (figura 4.20).

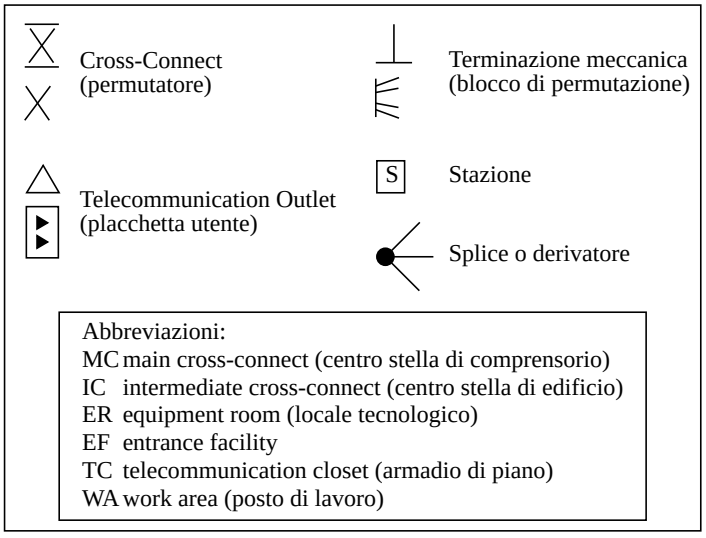


Fig. 4.20 - Simbologia ed abbreviazioni.

Essa deve comprendere:

- il disegno logico dell'intero comprensorio o del singolo edificio (figura 4.21);
- una tabella per identificare le dorsali;
- una tabella di armadio che indichi le connessioni tra l'armadio di piano e i posti di lavoro.

La tabella di documentazione delle dorsali deve contenere:

- gli identificativi di tutti i cavi ed il loro corrispondente numero di coppie o fibre;
- la localizzazione e l'identificativo dei due armadi a cui ogni cavo è attestato.

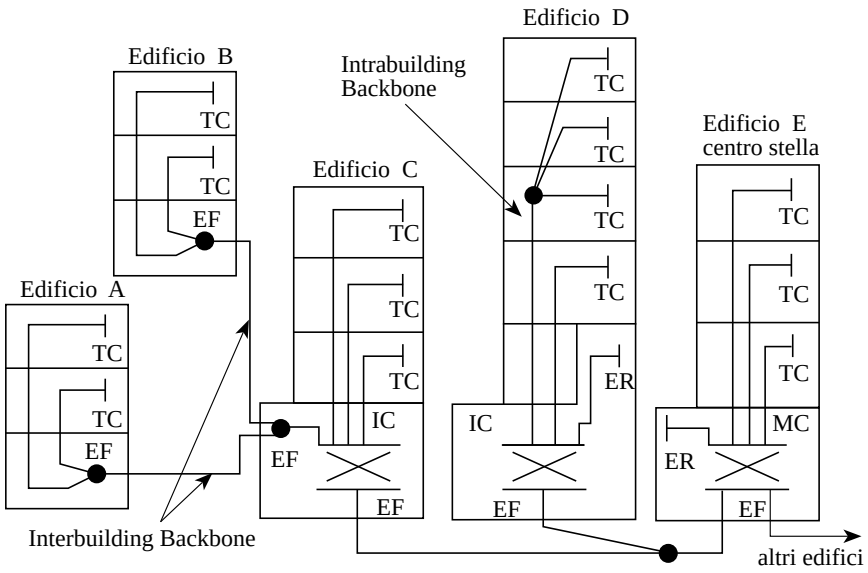


Fig. 4.21 - Esempio di progetto logico.

Ogni armadio di piano deve contenere la documentazione ad esso relativa in un apposito vano. Tale documentazione consiste in una tabella delle permutazioni, tramite cui è possibile ricostruire il percorso del cavo che, partendo da una certa posizione del permutatore, raggiunge il posto di lavoro; vanno inoltre indicate le coppie attive ed il loro utilizzo. La figura 4.22 e la tabella 4.4 mostrano rispettivamente un esempio di identificazione di un cavo entro un armadio e di tabella delle permutazioni.

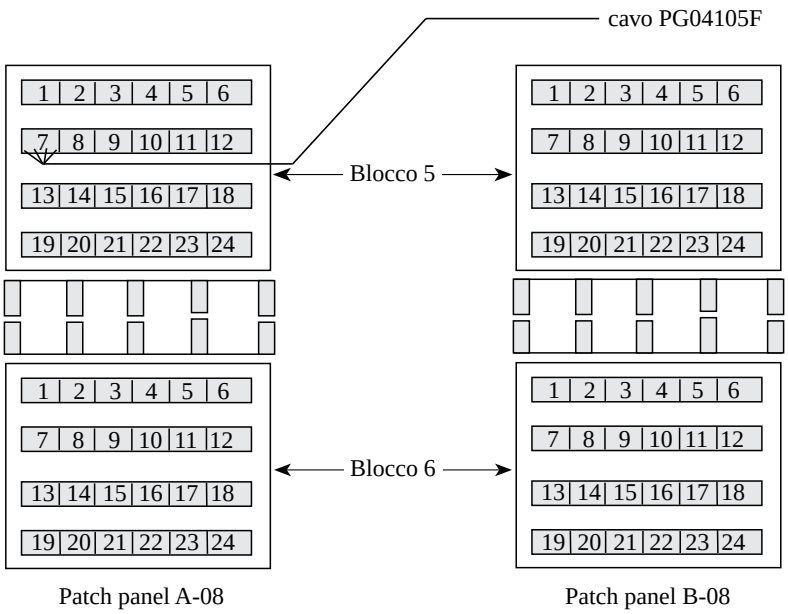


Fig. 4.22 - Identificazione di un cavo in un permutatore.

Posto lavoro	Patch panel	Blocco #	Posizione	Coppie attive	Tipo di utilizzo
PG04102F	A-08	05	04	2 e 3	Ethernet
PG04103F	A-08	05	05	2 e 3	Ethernet
PG04104F	A-08	05	06	1	Telefono
PG04105F	A-08	05	07	2 e 3	Ethernet
-	-	-	-	-	-
-	-	-	-	-	-
PG04110F	A-08	05	24	1	Telefono
-	-	-	-	-	-
-	-	-	-	-	-
PG04127F	A-08	06	19	2 e 3	Ethernet
PG04128F	A-08	06	20	1	Telefono
PG04129F	A-08	06	21	1	Telefono
PG04130F	A-08	06	22	1	Telefono

Tab. 4.4 - Esempio di tabella delle permutazioni.

4.4.9 Tipi di connettori e giunzioni

I connettori ammessi sono i seguenti:

- il connettore RJ45 per i cavi UTP a 4 coppie;
- il connettore ermafrodita per i cavi STP a 2 coppie;
- il connettore "N" per i cavi coassiali di dorsale;
- il connettore "BNC" per i cavi coassiali di distribuzione orizzontale;
- un connettore per fibra ottica in grado di sopportare almeno 200 cicli di estrazione/inserzione senza introdurre attenuazioni superiori a 1 dB; normalmente quello utilizzato è il tipo "ST";
- gli splices che servono per giuntare la fibra ottica; l'attenuazione massima ammessa sulla giunzione è di 0.3 dB.

4.5 LA BOZZA ISO/IEC DIS 11801

4.5.1 Introduzione

L'ISO/IEC DIS 11801 è una proposta di standard internazionale per i cablaggi ed è simile allo standard americano EIA/TIA 568, ma si differenza da questo per i seguenti motivi:

- ha una nomenclatura leggermente diversa;
- introduce il concetto di classi di lavoro;
- fornisce un maggior numero di dati sulle caratteristiche dei mezzi trasmissivi;
- permette l'utilizzo di un maggior numero di tipi di doppini e fibre ottiche, ma non ammette l'uso di cavi coassiali;
- introduce test più rigorosi per controllare le categorie dei cavi in rame;
- tratta in modo leggermente più approfondito gli aspetti della messa a terra;
- non si occupa di aspetti relativi alla documentazione.

Questa proposta è stata approvata nel luglio del 1994, ma attualmente (luglio 1995) l'unico documento disponibile è quello antecedente la votazione che è identificato col nome ISO/IEC DIS 11801, dove DIS significa Draft International Standard.

4.5.2 Diversità di nomenclatura

Gli elementi facenti parti di un cablaggio sono gli stessi indicati nello standard EIA/TIA 568, ma assumono a volte nomi diversi:

- il *Campus Distributor* (CD): è il permutatore principale dell'intero comprensorio ed equivale al main crossconnect;
- il *Building Distributor* (BD): è il permutatore principale del singolo edificio, ed equivale all'intermediate crossconnect;
- il *Floor Distributor* (FD): è il permutatore di piano, ed equivale al telecommunication closet (armadio di piano).

4.5.3 Topologia e caratteristiche principali del cablaggio

La topologia è di tipo stellare gerarchico ed è possibile inoltre connettere opzionalmente cavi di dorsale tra livelli uguali di gerarchia. Questo permette di distribuire meglio i cavi e ridurre l'utilizzo dei cavedi montanti degli edifici. La figura 4.23 mostra la topologia e le relazioni tra i vari elementi.

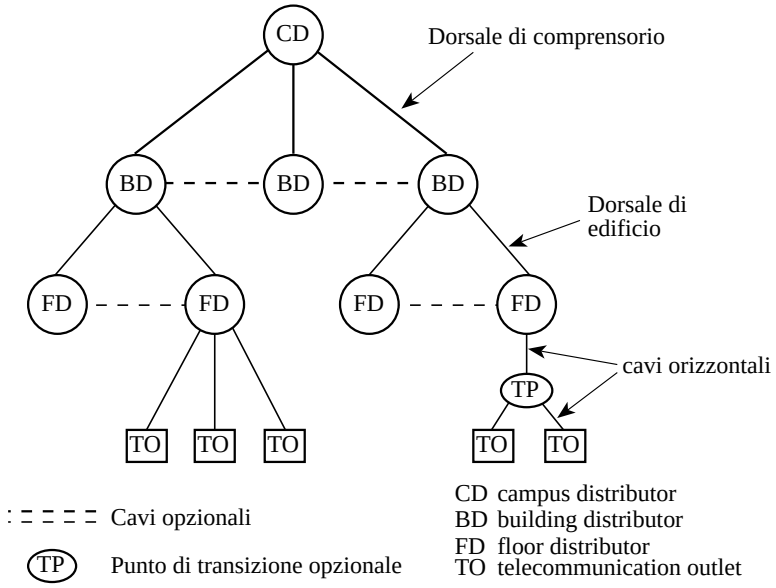


Fig. 4.23 - Il modello ISO/IEC DIS 11801.

Le distanze massime ammesse tra i vari elementi del cablaggio sono indicate nella figura 4.24.

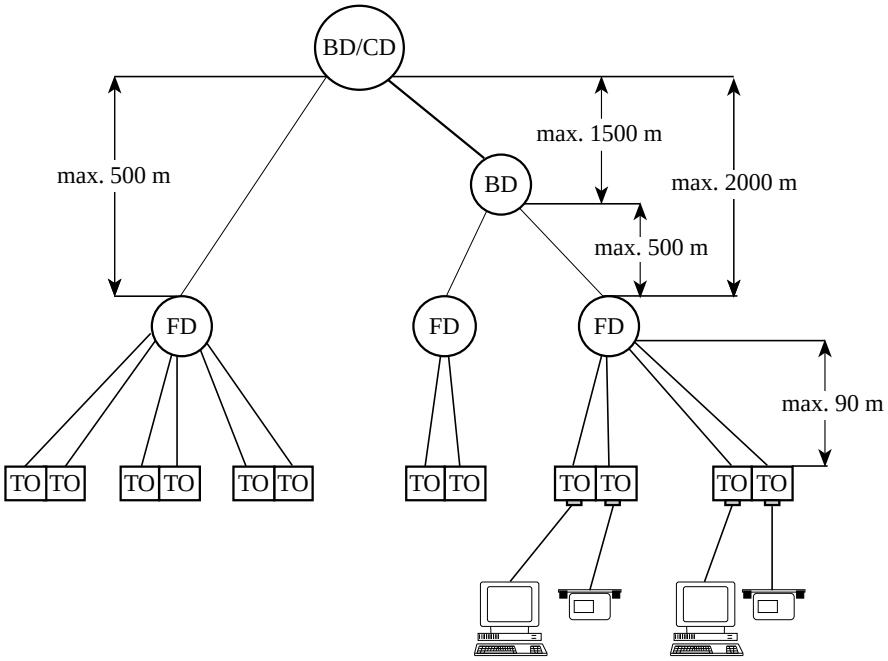


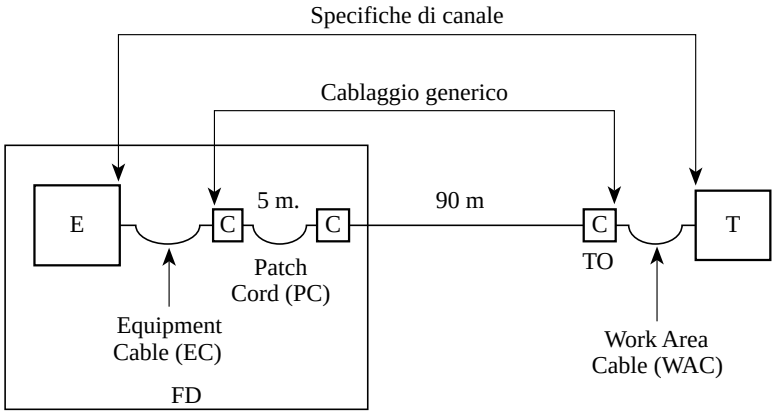
Fig. 4.24 - Topologia e limiti di distanze.

Le specifiche di canale sul cablaggio orizzontale stabiliscono uno sviluppo massimo di 95 m di cablaggio generico, al quale vanno sommati i cavetti di connessione degli apparati attivi per un totale di 100 m di cavo (figura 4.25). Al modello di cablaggio generico fanno riferimento i valori dei parametri elettrici delle classi di connessione (si veda il paragrafo 4.5.6).

Per il cablaggio orizzontale devono essere previsti almeno due cavi per ogni posto di lavoro, che partono dall'armadio di piano e terminano nella presa a muro:

- il primo cavo deve essere di categoria 3 o superiore;
- il secondo cavo deve essere di categoria 5 o in alternativa può essere una fibra ottica multimodale 62.5/125 μm.

La presa a muro o placchetta utente deve avere delle targhette permanenti, visibili esternamente dall'utente, che servono per identificare i cavi. I balun e gli adattatori d'impedenza devono essere esterni alla presa.



FD floor distributor (armadio di piano)
E equipment (apparecchiatura)
C connessione
T apparato terminale
TO telecommunication outlet (presa a muro)
ec cavo di connessione all'apparecchiatura
pc cavo di permutazione
wac cavo di connessione del posto di lavoro
ec + pc + wac ≤ 10 m

Fig. 4.25 - Cablaggio orizzontale.

4.5.4 I mezzi trasmissivi

Sulle dorsali sono ammessi i seguenti mezzi trasmissivi:

- fibre ottiche multimodali (62.5/125 μm preferita) e monomodali;
- cavi di tipo bilanciato (doppino) da 100 Ω (preferito), 120 Ω o 150 Ω che possono essere di tipo schermato o non schermato e possono essere composti da 2 o più coppie.

Per le dorsali è preferibile utilizzare fibre ottiche.

Sulla distribuzione orizzontale sono ammessi i seguenti mezzi trasmissivi:

- fibre ottiche multimodali (62.5/125 μm preferita);
- cavi di tipo bilanciato (doppino) da 100 Ω (preferito), 120 Ω o 150 Ω che possono essere di tipo schermato o non schermato e possono essere composti da 2 o più coppie.
- cavi ibridi, ovvero composti da elementi di diverso tipo o categoria, ad esempio: 4 coppie UTP da 100 Ω di Cat. 5 e 2 fibre ottiche.

I cavi di tipo bilanciato (doppini) da 100 Ω hanno le stesse caratteristiche

elettriche delle categorie 3, 4 e 5 (si vedano le tabelle 3.4 e 3.5), ad eccezione dei cavi schermati a cui sono state aggiunte alcune caratteristiche elettriche in relazione alla presenza dello schermo. Un parametro importante per i cavi schermati è l'impedenza di trasferimento che indica l'efficacia della schermatura; la tabella 4.5 mostra i valori richiesti dallo standard.

Caratteristiche del cavo			Categoria del cavo		
Caratteristiche elettriche @ 20 °C	Unità di misura	MHz	3	4	5
Massima impedenza di trasferimento	mΩ/m	1 10	50 100	50 100	50 100

Tab. 4.5 - Impedenza di trasferimento dei cavi schermati da 100 Ω.

I cavi di tipo bilanciato (doppini) da 120 Ω hanno le stesse caratteristiche di diafonia ed impedenza di trasferimento di quelli da 100 Ω, mentre le altre caratteristiche elettriche sono indicate nella tabella 4.6.

Caratteristiche del cavo			Categoria del cavo		
Caratteristiche elettriche @ 20 °C	Unità di misura	MHz	3	4	5
Impedenza	Ω	0.064 1÷100	125 ± 45 125 ± 15	125 ± 45 125 ± 15	125 ± 45 125 ± 15
Attenuazione massima ammessa	dB/100 m	0.064 0.256 0.512 0.772 1 4 10 16 20 31.25 62.5 100	non definita non definita non definita non definita non definita non definita non definita non definita - - - -	0.8 1.1 1.5 1.7 2 4 6.7 8.1 9.2 - - -	0.8 1.1 1.5 1.7 1.8 3.6 5.2 6.2 7 8.8 12.5 17

Tab. 4.6 - Caratteristiche elettriche dei cavi a 120 Ω.

I cavi STP con impedenza di 150 Ω devono avere le caratteristiche elettriche indicate nella tabella 4.7 e nella tabella 4.8.

Caratteristiche del cavo			Cavo STP a 150 Ω
Caratteristiche elettriche @ 20°C	Unità di misura	MHz	
Impedenza	Ω	1÷100	150 ± 15
Massima capacità tra una coppia sbilanciata e la terra	pf/100 m	0.001	100
Massima impedenza di trasferimento	mΩ/m	1 10	50 100
Velocità di propagazione minima			0.6 c
Massimo valore di resistenza	Ω/100 m		6
Attenuazione massima ammessa	dB/100 m	4 10 16 20 31.25 62.5 100	2.2 3.6 4.4 4.9 6.9 9.8 12.3

Tab. 4.7 - Diafonia dei cavi a 150 Ω.

Caratteristiche del cavo			Cavo STP a 150 Ω
Caratteristiche elettriche @ 20 °C	Unità di misura	MHz	
Near End Crosstalk (NEXT), minimo valore ammesso	dB @ 100 m	4 10 16 20 31.25 62.5 100	58 53 50 49 46 41 38

Tab. 4.8 - Caratteristiche elettriche dei cavi a 150 Ω.

La fibra ottica preferita è quella multimodale 62.5/125 μm, per la quale sono richieste le caratteristiche minime riportate nella tabella 4.9.

Lunghezza d'onda (nm)	Attenuazione massima (dB/Km)	Banda passante (MHz · Km)
850	3.5	200
1300	1.0	500

Tab. 4.9 - Caratteristiche della fibra 62.5/125 μm.

Un link in fibra ottica comprende le seguenti parti: il cavo in fibra ottica, i cavi di permutazione, gli eventuali giunti o splice, i connettori, i pannelli di permutazione. La massima attenuazione ammessa in un link è di 11 dB. La tabella 4.10 indica il caso peggiore di attenuazione in relazione al tipo di link ed alla lunghezza d'onda.

Sottosistema di cablaggio	Lunghezza del link	Attenuazione (dB)	
		850 nm	1300 nm
Orizzontale	100 m	2.5	2.3
Dorsale di edificio	500 m	3.8	2.8
Dorsale di comprensorio	1500 m	7.4	4.4

Tab. 4.10 - Attenuazione dei sottosistemi di cablaggio in fibra ottica.

4.5.5 Elementi di connessione (connecting hardware)

Nel cablaggio di distribuzione orizzontale ci sono almeno quattro punti di connessione che vengono realizzati con degli elementi indicati generalmente come *connecting hardware*; si tratta degli accoppiamenti presa-connettore (si veda la figura 4.26).

Il connecting hardware introduce una ridotta attenuazione aggiuntiva sulla connessione tra due apparati attivi (principalmente dovuta all'inevitabile discontinuità dell'impedenza, e quindi al return loss, descritto nel paragrafo 3.2.5), ma aumenta in modo considerevole la diafonia. I valori di attenuazione e diafonia (NEXT) dei componenti per i cablaggi a 100 Ω e 120 Ω sono indicati nelle tabelle 4.11 e 4.12, mentre quelli per i cablaggi a 150 Ω sono indicati nelle tabelle 4.13 e 4.14.

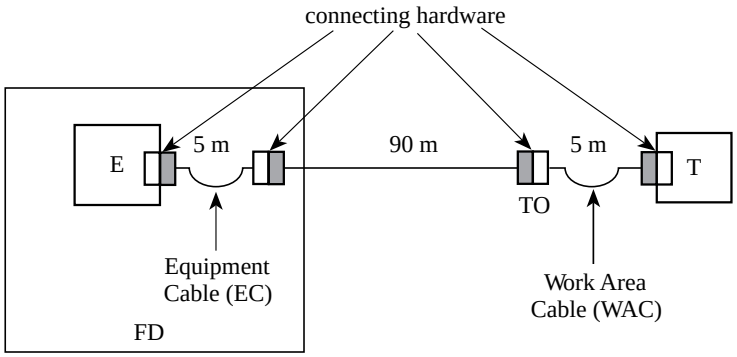


Fig. 4.26 - Elementi di connessione di un cablaggio.

Caratteristiche del connecting hardware per i cablaggi a 100 Ω o 120 Ω			Categoria del connecting hardware		
Caratteristiche elettriche	Unità di misura	MHz	3	4	5
Attenuazione massima, ammessa	dB	1	0.4	0.1	0.1
		4	0.4	0.1	0.1
		10	0.4	0.1	0.1
		16	0.4	0.2	0.2
		20	-	0.2	0.2
		31.25	-	-	0.2
		62.5	-	-	0.3
		100	-	-	0.4

Tab. 4.11 - Attenuazione del connecting hardware a 100 Ω e 120 Ω.

Caratteristiche del connecting hardware per i cablaggi a 100 Ω o 120 Ω			Categoria del connecting hardware		
Caratteristiche elettriche	Unità di misura	MHz	3	4	5
Near End Crosstalk (NEXT), minimo valore ammesso	dB	1	58	>65	>65
		4	46	58	>65
		10	38	50	60
		16	34	46	56
		20	-	44	54
		31.25	-	-	50
		62.5	-	-	44
		100	-	-	40

Tab. 4.12 - Diafonia (NEXT) del connecting hardware a 100 Ω e 120 Ω.

Caratteristiche del connecting hardware per i cablaggi schermati a 150 Ω			
Caratteristiche elettriche	Unità di misura	MHz	Cat. 5
Attenuazione massima, ammessa	dB	1	0.05
		4	0.05
		10	0.10
		16	0.15
		20	0.15
		31.25	0.15
		62.5	0.20
		100	0.25

Tab. 4.13 - Attenuazione del connecting hardware a 150 Ω.

Caratteristiche del connecting hardware per i cablaggi schermati a 150 Ω			
Caratteristiche elettriche	Unità di misura	MHz	Cat. 5
Near End Crosstalk (NEXT), minimo valore ammesso	dB	1	>65
		4	>65
		10	>65
		16	62.4
		20	60.5
		31.25	56.6
		62.5	50.6
		100	46.5

Tab. 4.14 - Diafonia (NEXT) del connecting hardware a 150 Ω.

Durante la realizzazione dei cavetti di connessione o permutazione (patch cord, equipment cable e work area cable), è necessario prestare molta cura nell'intestare il cavo sul connettore (plug) RJ45 per mantenere le caratteristiche di categoria 5. L'operazione richiede quattro fasi:

- spelare e preparare il cavo come indicato nella figura 4.27a;
- tagliare e disporre i conduttori come indicato nella figura 4.27b;
- inserire i conduttori nel connettore come indicato nella figura 4.27c;
- crimpare il connettore e controllare che il cavo riprenda la sua forma originale a 6 mm dal bordo esterno come indicato nella figura 4.27c.

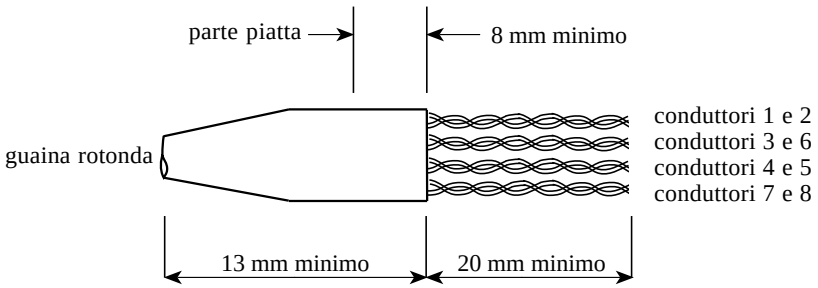


Fig. 4.27a - Spelatura e preparazione del cavo.

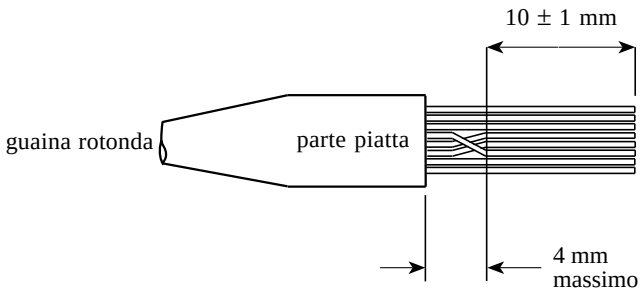


Fig. 4.27b - Disposizione dei conduttori.

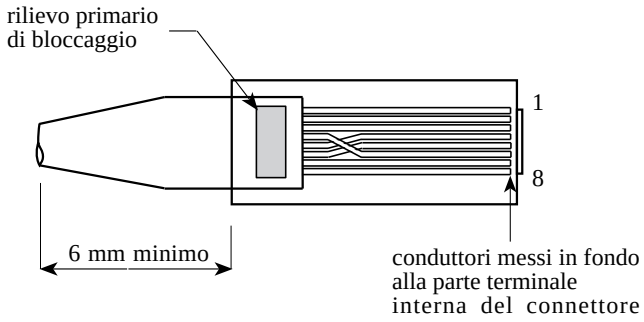


Fig. 4.27c - Inserzione dei conduttori nel connettore.

4.5.6 Classificazione delle connessioni

Sono state definite cinque classi di connessioni (link), di cui quattro classi per i cavi in rame ed una classe per la fibra ottica:

- classe A adatta per applicazioni fino a 100 kHz;
- classe B adatta per applicazioni fino a 1 MHz;
- classe C adatta per applicazioni fino a 16 MHz;
- classe D adatta per applicazioni fino a 100 MHz.

La fibra ottica non costituisce generalmente un limite per la banda passante delle apparecchiature utilizzate in un cablaggio.

La classe di connessione definisce le caratteristiche elettriche più importanti quali attenuazione, diafonia, ACR, riferite all'insieme di tutti i componenti passivi interposti tra due apparati attivi di telecomunicazione.

L'attenuazione totale di una connessione è data dalla somma dei valori di attenuazione di tutti i singoli componenti passivi: cavo di distribuzione orizzontale, connecting hardware, cavetti di connessione.

I cavetti di connessione, quali patch cord, equipment cable e work area cable, vengono normalmente realizzati con conduttori di tipo trefolato per renderli più flessibili, in questo caso l'attenuazione del cavo aumenta del 50% rispetto ad un cavo di equivalente categoria con conduttori solidi.

La diafonia totale di una connessione è la combinazione di quella di tutti i componenti ed i cavi interposti tra due apparati attivi.

La normativa stabilisce dei limiti per l'attenuazione e la diafonia (NEXT) riferiti al modello di cablaggio generico (si veda la figura 4.25). Le tabelle 4.15 e 4.16 mostrano rispettivamente i limiti per le quattro classi di connessione.

Frequenza MHz	Attenuazione massima ammessa (dB)			
	Classe A	Classe B	Classe C	Classe D
0.1	16	5.5	N/A	N/A
1	N/A	15	3.7	2.5
4	N/A	N/A	6.6	4.8
10	N/A	N/A	10.75	7.5
16	N/A	N/A	14	9.4
20	N/A	N/A	N/A	10.5
31.25	N/A	N/A	N/A	13.1
62.5	N/A	N/A	N/A	18.4
100	N/A	N/A	N/A	23.2

Tab. 4.15 - Attenuazione delle classi di connessione

I link realizzati con i cavi di rame devono rispondere a determinati requisiti di qualità trasmissiva, che si esprime col valore di ACR. Tale valore indica il rapporto tra il segnale attenuato, all'estremità di una connessione dove è situato il ricevitore, ed il segnale indotto dalla coppia vicina per effetto della diafonia (si veda il paragrafo 3.2.5).

La normativa stabilisce soltanto i valori di ACR per la connessione di classe D. Si noti che, per ottenere i valori indicati nella tabella 4.17, può non essere sufficiente soddisfare i limiti di attenuazione e di diafonia indicati nelle tabelle 4.15 e 4.16. La normativa demanda a chi progetta i componenti del cablaggio il compito di decidere quali valori migliorare per rientrare nei limiti di ACR.

Frequenza MHz	Valori minimi di NEXT loss (dB)			
	Classe A	Classe B	Classe C	Classe D
0.1	27	48	N/A	N/A
1	N/A	11	39	54
4	N/A	N/A	29	45
10	N/A	N/A	23	39
16	N/A	N/A	19	36
20	N/A	N/A	N/A	34.5
31.25	N/A	N/A	N/A	31.5
62.5	N/A	N/A	N/A	27
100	N/A	N/A	N/A	24

Tab. 4.16 - Diafonia (NEXT) delle classi di connessione

Frequenza (MHz)	ACR minimo (dB) Classe D
1	-
4	40
10	35
16	30
20	28
31.25	23
62.5	13
100	4

Tab. 4.17 - Valori minimi di ACR per la connessione di classe D.

Per esempio, se si considera una tipica connessione tra due apparati attivi (si veda la figura 4.26) composta da un cablaggio di 90 m, realizzato con cavo e connecting hardware di categoria 5, e due cavetti di categoria 5 (tipo flessibile con conduttori trefolati) per l'interconnessione degli apparati, si ottengono un valore teorico di attenuazione a 100 MHz di 24.37 dB e un valore teorico di diafonia (NEXT) a 100 MHz di 29.3 dB (contro i 23.2 dB e 24 dB delle tabelle 4.15 e 4.16), per un valore risultante di ACR di 4.93 dB.

4.5.7 Trattamento degli schermi e messa a terra

Gli schermi dei cavi, gli apparati e gli armadi di piano devono essere collegati all'impianto di terra dell'edificio che deve essere realizzato in conformità alle vigenti normative sulla sicurezza degli impianti elettrici. I collegamenti di terra devono essere permanenti e continui. Deve inoltre essere garantita una continuità elettrica dello schermo lungo tutto il percorso tra due apparati attivi, anche quando si passa attraverso dei punti di permutazione. Tutti gli elettrodi di terra di un edificio devono essere connessi tra loro con un cavo opportuno per garantire una equipotenzialità dei punti di terra. L'impianto di terra dell'edificio deve garantire una differenza di potenziale inferiore a 1 V r.m.s. tra due punti qualunque di connessione. Se i requisiti citati non possono essere mantenuti bisogna usare la fibra ottica per eliminare i rischi di elevata corrente di terra lungo lo schermo dei cavi.

4.5.8 Connettori per fibre ottiche

I connettori utilizzabili per la terminazione delle fibre ottiche sono di due famiglie:

- connettori "ST" simplex o duplex: hanno una chiave d'inserzione e si bloccano mediante un meccanismo a baionetta;
- connettori "SC" simplex o duplex: sono molto simili ai precedenti, hanno una chiave d'inserzione, ma sono inseribili e disinseribili a pressione.

La figura 4.28 mostra i tipi di connettori utilizzabili.

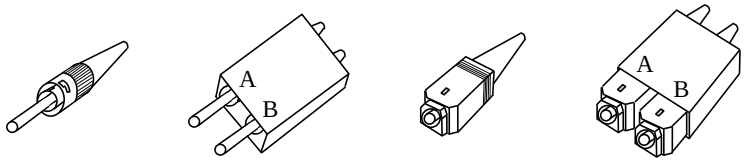


Fig. 4.28 - Tipi di connettori per fibra ottica utilizzabili.

Il pannellino della placchetta utente deve poter ospitare due bussole di tipo simplex o una di tipo duplex; inoltre deve riportare due lettere alfabetiche visibili, A e B, che servono per identificare le fibre (si vedano le figure 4.29 e 4.30). Le bussole servono ad allineare meccanicamente coppie di connettori.

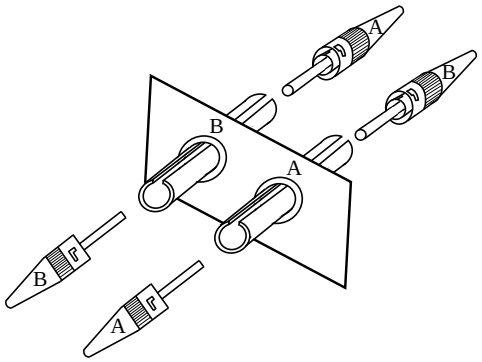


Fig. 4.29 - Pannellino per connettori ST.

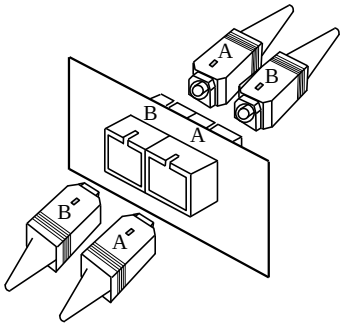


Fig. 4.30 - Pannellino per connettori SC.

4.6 LA PROPOSTA SP-2840-A

4.6.1 Introduzione

Lo SP-2840-A è una proposta di revisione dello standard americano EIA/TIA 568 che, dopo l'approvazione prevista per il mese di luglio del 1995, prenderà il nome di EIA/TIA-568-A. Questa revisione del precedente standard è motivata dalla necessità di avere dei cablaggi con prestazioni superiori e di stabilire quindi delle normative più adeguate ad una maggiore banda trasmissiva.

Il documento incorpora e sostituisce i bollettini: TSB36, TSB40, TSB40A e TSB53, che definivano le caratteristiche dei cavi e del connecting hardware riferite alle gategorie 3, 4 e 5 (100 Ω) e al tipo STP a 150 Ω; introduce inoltre delle nuove specifiche per i cablaggi in fibra ottica.

Questa normativa si differenzia da EIA/TIA 568 per i seguenti motivi principali:

- non ammette l'utilizzo di cavi coassiali;
- fornisce un maggior numero di dati sulle caratteristiche dei doppini e dei componenti passivi;
- definisce il modello di connessione;
- definisce le specifiche per il cablaggio in fibra ottica;
- permette l'uso di fibre ottiche monomodali sulle dorsali.

4.6.2 I doppini ed il connecting hardware

I doppini a 100 Ω hanno le caratteristiche già descritte nel paragrafo 3.2.9; i cavi chiamati STP-A 150 Ω hanno le stesse caratteristiche, fino a 100 MHz, di quelli definiti da ISO/IEC DIS 11801 (si vedano le tabelle 4.7 e 4.8), con la differenza che devono essere provati fino a 300 MHz.

Il connecting hardware (accoppiamento presa-connettore) a 100 Ω o 150 Ω deve avere le stesse caratteristiche richieste da ISO/IEC DIS 11801 (si vedano le tabelle 4.11, 4.12, 4.13 e 4.14) per le frequenze fino a 100 MHz, ma la componentistica a 150 Ω viene collaudata fino a 300 MHz.

I cavetti di connessione, che prendono il nome generico di patch cord, vengono normalmente realizzati con conduttori di tipo trefolato per renderli più flessibili. Nella proposta SP-2840-A si suppone che l'attenuazione del cavo aumenti del 20% rispetto ad un cavo di equivalente categoria con conduttori solidi, mentre nell'ISO/IEC DIS 11801 si ipotizza un aumento di attenuazione del 50%.

I cavetti di connessione devono essere attestati sui connettori RJ45 nello stesso modo indicato da ISO/IEC DIS 11801 (si veda il paragrafo 4.5.5).

4.6.3 Modello di connessione

Il modello di connessione è utilizzato come riferimento per le tabelle di attenuazione e diafonia (NEXT) ed è costituito da 90 m di cablaggio orizzontale, i connecting hardware, il permutatore di armadio ed un massimo di 10 m a disposizione per i cavetti di permutazione (si veda la figura 4.31).

Le tabelle 4.18 e 4.19 riportano rispettivamente i valori massimi di attenuazione e quelli minimi di diafonia (NEXT) che sono da intendere come valore di *channel performance*, ovvero prestazione minima richiesta riferita al modello di connessione.

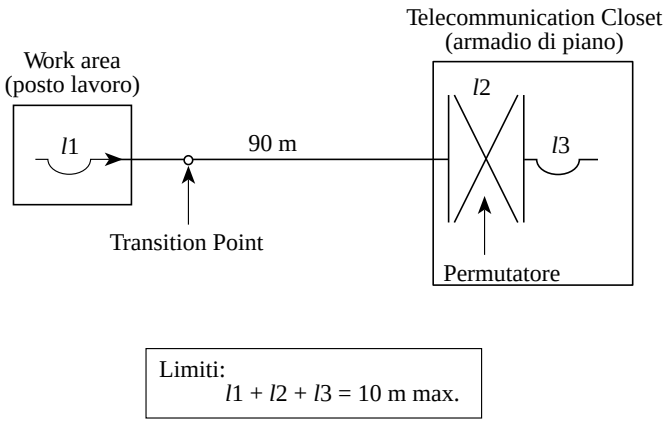


Fig. 4.31 - Modello di connessione.

Frequenza MHz	Attenuazione massima ammessa (dB)		
	Categoria 3	Categoria 4	Categoria 5
1	4.2	2.6	2.5
4	7.3	4.8	4.5
8	10.2	6.7	6.3
10	11.5	7.5	7.0
16	14.9	9.9	9.2
20	-	11.0	10.3
25	-	-	11.4
31.25	-	-	12.8
62.5	-	-	18.5
100	-	-	24.0

Tab. 4.18 - Valori massimi di attenuazione del modello di connessione.

La normativa non stabilisce i valori di ACR, ma suggerisce di considerare il valore richiesto dai singoli standard trasmissivi. Normalmente il valore di ACR è compreso tra i 14.5 dB richiesti da 10BaseT sui cavi UTP a 4 coppie e 21.1 dB richiesti dallo standard TP-PMD (FDDI) a 10 MHz e 31.25 MHz rispettivamente; lo standard 802.5 chiama questo valore col nome di NIR (*NEXT to Insertion loss Ratio*) ed i valori richiesti sono riportati nel paragrafo 7.6.2.

Frequenza MHz	Valori minimi di NEXT loss (dB)		
	Categoria 3	Categoria 4	Categoria 5
1	39.1	53.3	60.3
4	29.3	43.3	50.6
8	24.3	38.2	45.6
10	22.7	36.6	44.0
16	19.3	33.1	40.6
20	-	31.4	39.0
25	-	-	37.4
31.25	-	-	35.7
62.5	-	-	30.6
100	-	-	27.1

Tab. 4.19 - Valori minimi di diafonia (NEXT) del modello di connessione.

4.6.4 Cablaggio in fibra ottica

La necessità di maggiore velocità trasmissiva pone il problema di come predisporre un cablaggio. Gli standard trasmissivi con maggiori prestazioni sono nati prima su fibra ottica e poi, con non poche difficoltà, sono stati resi disponibili anche su cavi in rame. Sono passati non meno di tre anni da quando sono stati disponibili i primi apparati FDDI su fibra ottica a quando sono stati disponibili quelli su cavo UTP. Con le attuali tecniche disponibili e la riduzione dei costi sulla fibra ottica e della componentistica in genere, si può pensare di portare la fibra ottica al posto di lavoro in quelle realtà dove si ha una veloce evoluzione verso i sistemi trasmissivi ad alte prestazioni. La soluzione è un compromesso tra le prestazioni richieste nel presente e nell'immediato futuro ed i costi di realizzazione.

L'unica bozza di standard che affronta in modo dettagliato il cablaggio in fibra ottica è la SP-2840-A.

I connettori ammessi sono gli stessi definiti da ISO/IEC DIS 11801 (si veda la figura 4.28).

La placchetta a muro, o una coppia di connettori facenti parti di un pannello di terminazione, devono essere realizzati nel modo indicato nelle figure 4.29 e 4.30; le targhette "A" e "B" servono per facilitare il compito di chi deve effettuare le connessioni tra gli apparati attivi ed il cablaggio.

Il montaggio dei connettori, sia esso su placchetta a muro o su pannello, deve essere effettuato nei modi indicati nella figura 4.32.

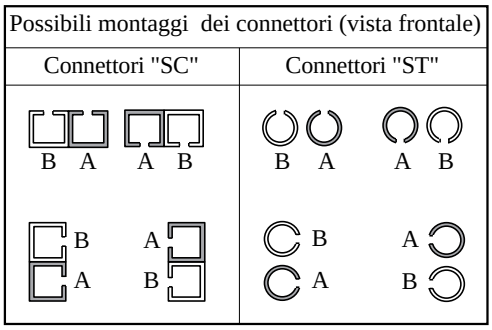


Fig. 4.32 - Montaggi dei connettori per fibre ottiche.

Il cablaggio orizzontale in fibra ottica deve avere una lunghezza massima di 90 m e deve essere realizzato con una bifibra.

Una dorsale in fibra ottica deve essere connettorizzata ai due estremi su due pannelli di terminazione e la numerazione da applicare alle fibre è quella indicata nella figura 4.33.

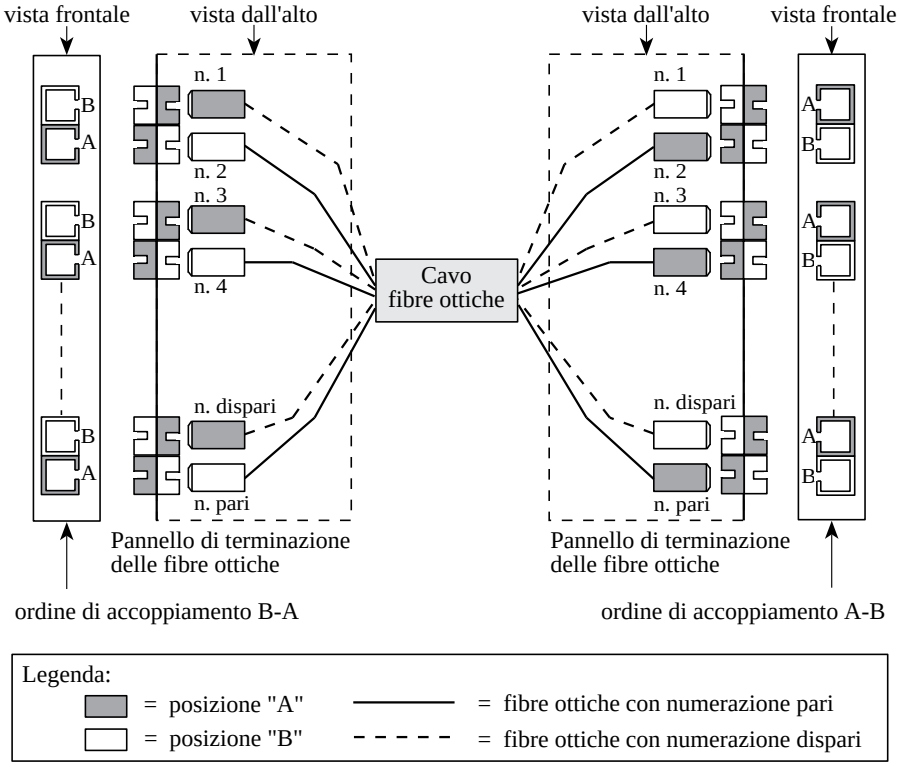


Fig. 4.33 - Dorsale in fibra ottica attestata sui pannelli di terminazione.

Il cablaggio in fibra ottica deve essere organizzato nel modo indicato nella figura 4.34.

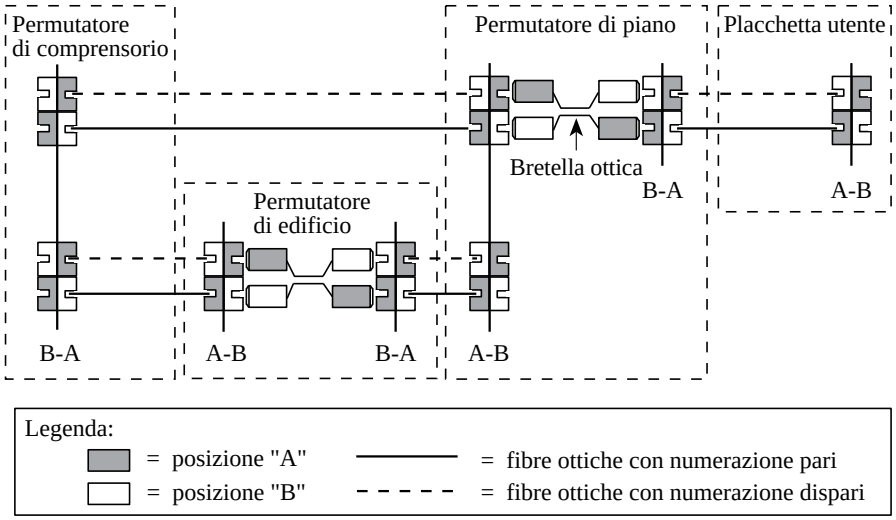


Fig. 4.34 - Cablaggio in fibra ottica.

Il cablaggio orizzontale in fibra ottica va certificato in modo semplice e poco costoso in quanto è sufficiente verificare che l'attenuazione massima della tratta da 90 m, compresa tra il pannello dell'armadio di distribuzione orizzontale e la placchetta a muro, sia a inferiore a 2 dB. Tale verifica va effettuata alla lunghezza d'onda di 850 nm e 1300 nm. Il modello di certificazione per il cablaggio orizzontale è quello indicato nella figura 4.35.

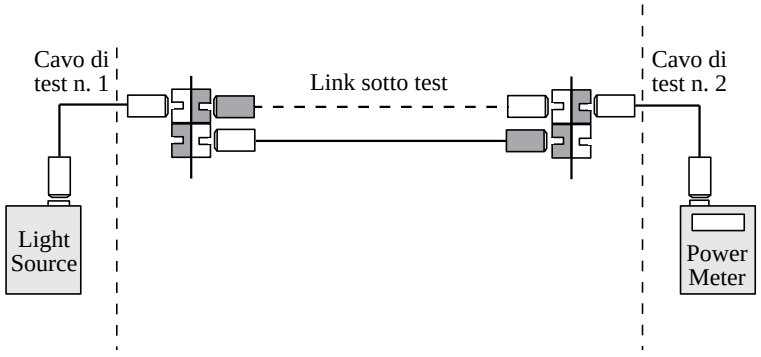


Fig. 4.35 - Modello di certificazione del cablaggio orizzontale in fibra ottica.

4.7 CERTIFICAZIONE DEI CABLAGGI

Un cablaggio di categoria 5 (definizione EIA/TIA SP-2840-A) o di classe D (definizione ISO/IEC DIS 11801) offre delle elevate prestazioni trasmissive, ma per definirsi tale va certificato con appositi strumenti di misura.

4.7.1 La proposta del gruppo di lavoro TR41.8.1

La normativa proposta dal gruppo di lavoro TR41.1.8 del comitato EIA/TIA prevede due configurazioni di test: il *basic link* (si veda la figura 4.36) ed il *channel* (si veda la figura 4.31).

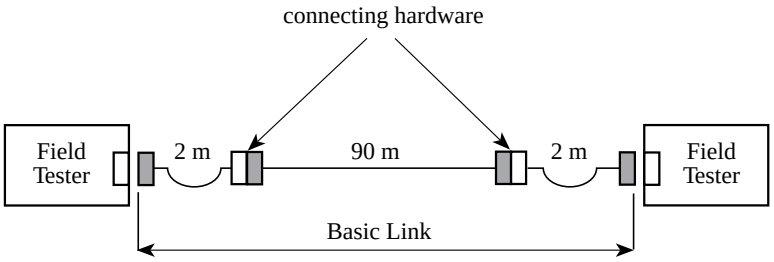


Fig. 4.36 - Modello basic link.

Prima di iniziare la certificazione bisogna conoscere la velocità di propagazione del cavo; nel caso non la si conosca, alcuni strumenti permettono di ricavarla calibrando lo strumento con uno spezzone di cavo di lunghezza nota.

A seconda che si verifichi il basic link o il channel, cambiano i limiti di attenuazione e diafonia (NEXT). Nel caso del channel i limiti sono quello indicati nelle tabelle 4.18 e 4.19; nel caso di basic link i limiti sono quelli indicati nelle tabelle 4.20 e 4.21.

In fase di certificazione bisogna effettuare la prova di *dual NEXT*. Si tratta di eseguire il test con il generatore da un lato del cavo e lo strumento di misura dall'altro, e poi scambiarli. Alcuni strumenti sono composti da due parti che contengono sia il generatore che lo strumento di misura, e permettono di effettuare il test senza dover scambiare i due elementi.

La differenza tra i due valori di NEXT misurati ai due estremi di un link è da attribuire principalmente alla differente qualità delle intestazioni di prese e connettori. Tale differenza può raggiungere i 4 dB, e ai fini del risultato va sempre considerato il valore peggiore.

Frequenza MHz	Attenuazione massima ammessa (dB)		
	Categoria 3	Categoria 4	Categoria 5
1	3.2	2.2	2.1
4	6.1	4.3	4.0
8	8.8	6.0	5.7
10	10.0	6.8	6.3
16	13.2	8.8	8.2
20	-	9.9	9.2
25	-	-	10.3
31.25	-	-	11.5
62.5	-	-	16.7
100	-	-	21.6

Tab. 4.20 - Valori massimi di attenuazione del basic link.

Frequenza MHz	Valori minimi di NEXT loss (dB)		
	Categoria 3	Categoria 4	Categoria 5
1	40.1	54.7	60
4	30.7	45.1	51.8
8	25.9	40.2	47.1
10	24.3	38.6	45.5
16	21.0	35.3	42.3
20	-	33.7	40.7
25	-	-	39.1
31.25	-	-	37.6
62.5	-	-	32.7
100	-	-	29.3

Tab. 4.21 - Valori minimi di diafonia (NEXT) del basic link.

La normativa stabilisce due classi di strumenti aventi due tipi di accuratezza:

- gli strumenti di livello 1 hanno un'accuratezza di ± 3.4 dB sulla misura di diafonia (NEXT) e ± 1.3 dB sulla misura di attenuazione;
- gli strumenti di livello 2 hanno un'accuratezza di ± 1.6 dB sulla misura di diafonia (NEXT) e di ± 1 dB sulla misura di attenuazione.

4.7.2 Interpretazione degli standard

Alcuni parametri di progetto imposti dagli standard, ed in particolare la massima lunghezza dei work area cable, sono definiti in funzione dei casi estremi, per esempio un link con cavo orizzontale di lunghezza massima (90 m). Tuttavia, con l'introduzione della misura del link, anche ai fini della certificazione l'aspetto fondamentale risulta essere quello delle caratteristiche elettriche del link complessivo su cui saranno collegate le apparecchiature attive, e non quelle delle sue singole parti.

Questa considerazione permette di adottare un'interpretazione elastica degli standard, spesso utile per risolvere problemi pratici e per contenere i costi. Per esempio, se i cavi orizzontali che servono una stanza sono molto al di sotto della lunghezza massima, e non è semplice distribuire le prese in modo uniforme, è possibile utilizzare work area cable anche ben più lunghi di 5 m, eventualmente ricorrendo a conduttori solidi e non trefolati per non degradare troppo le prestazioni.

4.8 LO STANDARD EIA/TIA 569

Il cablaggio strutturato comporta la posa di una considerevole quantità di cavi e l'installazione di armadi contenenti i pannelli di permutazione e le apparecchiature attive. Inoltre, in corrispondenza degli armadi di piano convergono i fasci di cavi dei cablaggi orizzontali, fasci che raggiungono diametri dell'ordine delle decine di centimetri. Tutto ciò crea seri problemi se l'edificio non è stato adeguatamente progettato. Lo standard EIA/TIA 569 definisce le caratteristiche minime per le infrastrutture edilizie degli edifici in cui devono essere installati sistemi di cablaggio strutturato secondo lo standard EIA/TIA 568. Si osservi che gli standard per i cablaggi strutturati prevedono che l'edificio sia in costruzione o in ristrutturazione, e che sia quindi possibile porre in atto i necessari interventi edilizi.

In figura 4.37 sono rappresentati i principali elementi di cui lo standard EIA/TIA 569 determina le caratteristiche, le possibili modalità costruttive ed i materiali impiegabili.

Il principale problema che si incontra normalmente nella realizzazione di un cablaggio strutturato è la inadeguatezza delle canalizzazioni per il cablaggio orizzontale. Esse devono poter ospitare un numero di cavi crescente man mano che ci si avvicina all'armadio di piano. Lo standard fornisce le seguenti indicazioni:

- si deve prevedere l'utilizzo di almento tre apparecchiature per posto di lavoro;
- si deve prevedere un posto di lavoro ogni 10 m^2 di spazio utilizzabile;
- si devono predisporre canaline per un totale di 650 mm^2 di sezione per ogni 10 m^2 di spazio servito.

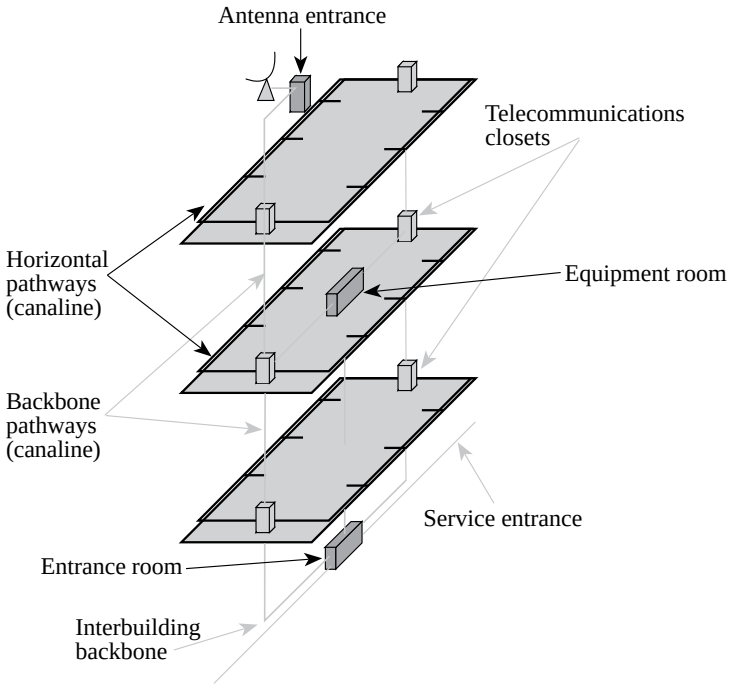


Fig. 4.37 - Principali elementi contemplati dallo standard EIA/TIA 569.

Inoltre, per garantire l'integrità dei cavi (doppini in particolare) dopo la posa, lo standard indica i minimi raggi di curvatura delle canaline, la massima distanza tra pozzetti o scatole accessibili lungo una canalina, e il massimo numero di cavi ospitabili nei tubi, in funzione del diametro. Quest'ultima specifica è riportata in tabella 4.22.

Infine, vengono fornite alcune indicazioni sulle minime distanze ammesse tra cavi di segnale e linee di alimentazione elettrica, come riportato in tabella 4.23.

Diametro del tubo (mm)	Diametro dei cavi (mm)									
	3.3	4.6	5.6	6.1	7.4	7.9	9.4	13.5	15.8	17.8
15.8	1	1	0	0	0	0	0	0	0	0
20.9	6	5	4	3	2	2	1	0	0	0
26.6	8	8	7	6	3	3	2	1	0	0
35.1	16	14	12	10	6	4	3	1	1	1
40.9	20	18	16	15	7	6	4	2	1	1
52.5	30	26	22	20	14	12	7	4	3	2
62.7	45	40	36	30	17	14	12	6	3	3
77.9	70	60	50	40	20	20	17	7	6	6
90.1							22	12	7	6
102.3							30	14	12	7

Tab. 4.22 - Massimo numero di cavi ospitabili nei tubi.

Situazione	Distanza minima		
	< 2 kVA	2 - 5 kVA	> 5 kVA
Linee elettriche non schermate in prossimità di canaline aperte o non metalliche	127 mm	305 mm	610 mm
Linee elettriche non schermate in prossimità di canaline metalliche con collegamento di terra	64 mm	152 mm	305 mm
Linee elettriche schermate in prossimità di canaline metalliche con collegamento di terra	-	76 mm	152 mm

Tab. 4.23 - Minime distanze ammesse tra cavi di segnale e linee di alimentazione elettrica.

4.9 LO STANDARD TIA/EIA 607

Lo standard TIA/EIA 607 affronta il problema di fornire una rete di messa a terra (*grounding* o, più propriamente, *earthing*) e di collegamento delle masse elettriche (*bonding*) aggiuntiva rispetto a quella per le alimentazioni elettriche e dedicata al sistema di cablaggio. Lo schema di base di tale rete è riportato in figura 4.38.

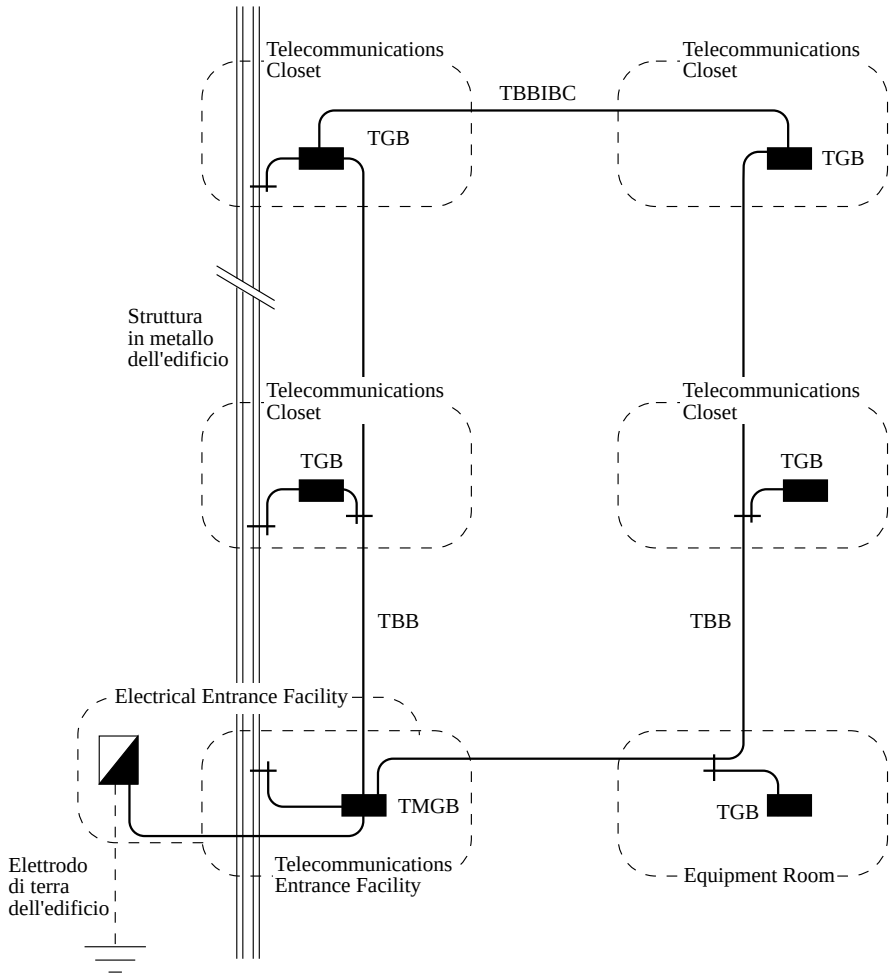


Fig. 4.38 -Rete di bonding e grounding

Gli elementi previsti, le cui caratteristiche minime sono indicate nello standard, sono i seguenti:

- *Telecommunications Main Grounding Busbar* (TGMB), barra in rame per il collegamento a bassissima impedenza delle dorsali di terra del cablaggio con il sistema di messa a terra dell'edificio;
- *Telecommunications Grounding Busbar* (TGB), barra in rame per il collegamento a bassissima impedenza dell'utenza nel telecommunications closet (strutture metalliche dei rack, quadri di alimentazione elettrica, ecc.) con la dorsale di terra del cablaggio;

- *Telecommunications Bonding Backbone* (TBB), dorsale di terra e di collegamento delle masse elettriche dedicata al cablaggio; raggiunge tutti i telecommunications closet;
- *Telecommunications Bonding Backbone Interconnecting Bonding Conductor* (TBBIBC), collegamento tra i TGB dei telecommunication closet che eventualmente si trovano sul medesimo piano; deve essere presente nell'ultimo piano dell'edificio e ogni tre piani intermedi.

Tutti i conduttori di terra devono avere un diametro minimo di 6 AWG (circa 3.4 mm).

4.10 PARTICOLARITÀ DI ALCUNI SISTEMI DI CABLAGGIO

I sistemi di cablaggio che consideriamo in questo paragrafo sono tutti conformi allo standard EIA/TIA 568, ma si differenziano tra loro per l'appartenenza a due differenti famiglie, che sono:

- i sistemi di derivazione dati, i quali sono basati sulla permutazione effettuata tramite connettori RJ45. I principali sono: IBM ACS, Digital OPEN DECconnect, AMP ACO, MOD-TAP, Krone, Panduit;
- i sistemi di derivazione telefonica, i quali sono basati sulla permutazione di tipo telefonico. I principali sono: AT&T PDS, Northern Telecom IBDN, Krone, Trucco SCP.

La figura 4.39 e la figura 4.40 mostrano le differenze tra le due famiglie di cablaggi.

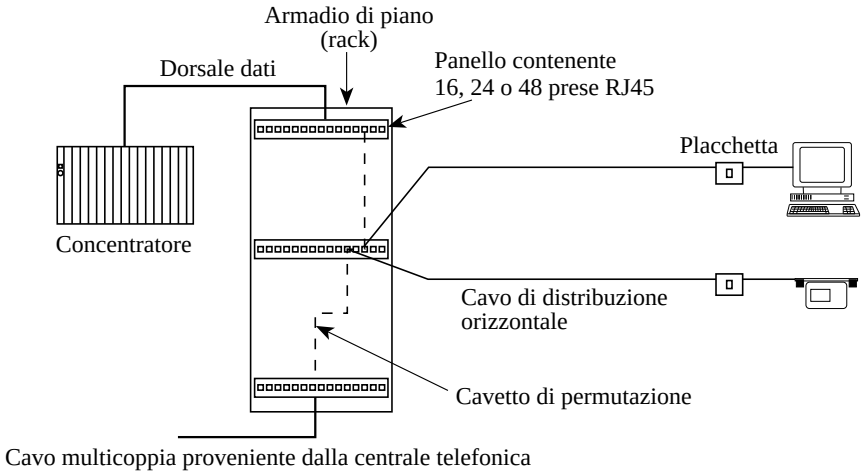


Fig. 4.39 - Cablaggio di derivazione dati.

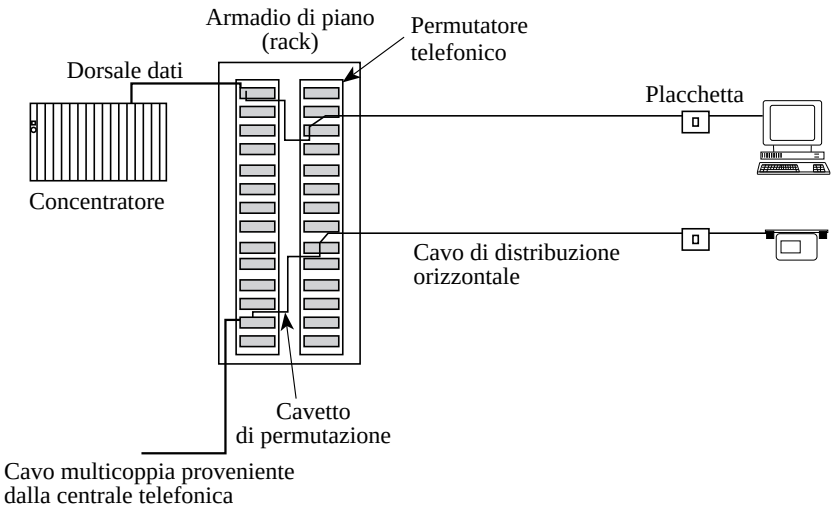


Fig. 4.40 - Cablaggio di derivazione telefonica.

4.10.1 Il sistema IBM/ACS

Il sistema ACS (Advanced Connectivity System) può ospitare sia cavi di tipo UTP che FTP, ma normalmente usa il secondo tipo, in quanto la IBM ha lunga tradizione nei cavi schermati ed inoltre ritiene che sia la migliore soluzione alle problematiche di suscettibilità ed emissione di disturbi elettromagnetici. I cavi utilizzati e tutta la componentistica passiva sono di categoria 5. La permutazione avviene su pannelli modulari contenenti un massimo di 48 prese RJ45 ciascuno. L'adattamento ai vari sistemi di telecomunicazione viene effettuato con appositi cavetti di permutazione che adattano sia le diverse tipologie di connettori e cavi, sia, quando necessario, l'impedenza. La figura 4.41 mostra un esempio di cablaggio ACS.

4.10.2 Il sistema Digital/Open DECconnect

Il sistema OPEN DECconnect della Digital Equipment è stato uno dei primi ad uniformarsi alle specifiche EIA/TIA 568. Esso utilizza un solo tipo di connettore (RJ45) per i due tipi di servizi fonia e dati. A discrezione dell'utente finale, si può scegliere se utilizzare una presa RJ45 con l'icona del telefono o con l'icona di trasmissione dati, per differenziare i due tipi di servizi. Il sistema di cablaggio è adatto

sia per i sistemi schermati sia per quelli non schermati e si possono quindi utilizzare cavi UTP o FTP. L'adattamento ai vari sistemi di telecomunicazione viene effettuato con appositi cavetti di permutazione che adattano sia le diverse tipologie di connettori e cavi, sia, quando necessario, l'impedenza. Lo schema di collegamento è molto simile a quello riportato nella figura 4.39.

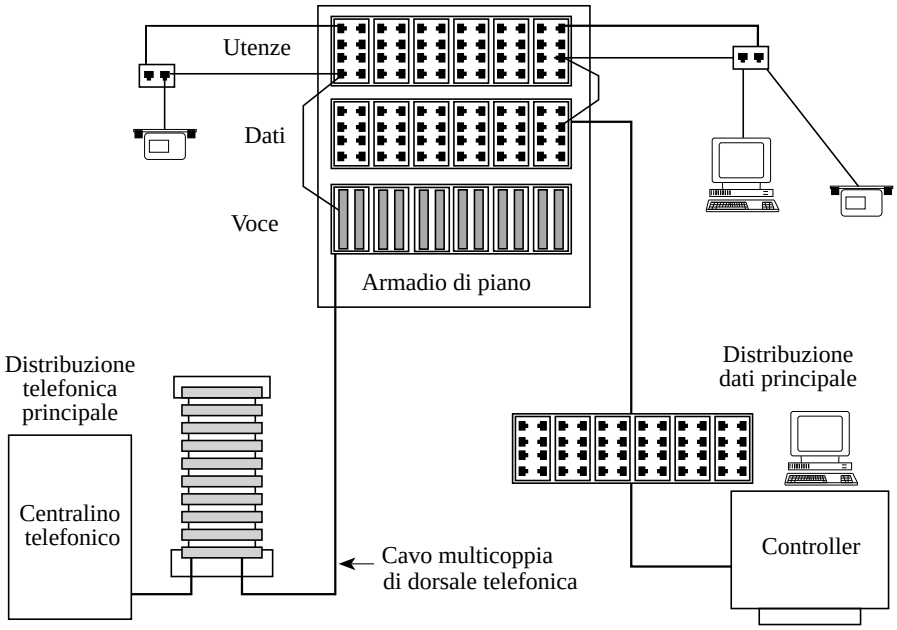


Fig. 4.41 - Esempio di cablaggio IBM ACS.

4.10.3 Il sistema AMP/ACO

Il sistema ACO (AMP Communication Outlet) dell'AMP può essere proprietario o standard, a seconda di come viene utilizzato. Esso è compatibile con il cabling system IBM e quindi può anche ospitare cavi STP di tipo 1 e 2; accetta inoltre cavi UTP e FTP da 100 Ω o 120 Ω. Questo cablaggio è modulare e molto flessibile, ed è composto da due elementi principali:

- la presa a muro, o placchetta utente, che a sua volta è composta da:
  - l'*housing*, che è l'elemento plastico dove vengono alloggiati l'edge connector ed il modulo di adattamento, che può essere ad una o due posizioni;
  - l'*edge-connector*, che permette la connessione tra il cavo ed il modulo;

- il *modulo*, che può contenere uno o due prese specifiche ed, a volte, un balun integrato;
- il *patch-panel*, che serve ad effettuare le permutazioni, dentro l'armadio, tra le dorsali dati o fonia e le utenze; esso ospita gli stessi housing della presa a muro e di conseguenza gli stessi moduli ed edge-connector.

I moduli si inseriscono nell'edge-connector tramite un circuito stampato. Essi possono contenere fino a due prese e sono in grado di ottimizzare l'utilizzo delle coppie. Si possono utilizzare ad esempio: moduli con due RJ45 cablati per Ethernet, due RJ11 cablati per avere due telefoni, due BNC da 93 Ω e relativi balun integrati per connettere due terminali IBM 3270, ecc.

La figura 4.42 mostra lo schema di collegamento.

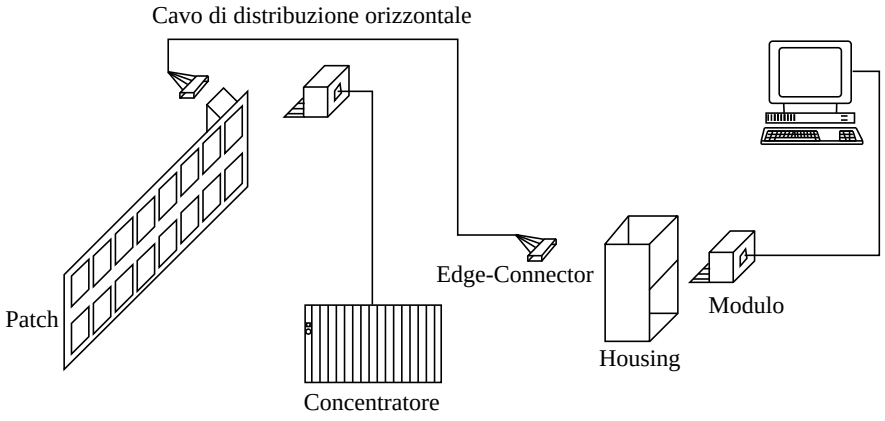


Fig. 4.42 - Esempio di cablaggio AMP ACO.

4.10.4 Il sistema AT&T/PDS

Il sistema PDS (Premise Distribution System) dell'AT&T è basato sulla permutazione telefonica; esso è costituito dai seguenti elementi principali: il wiring block, il connecting block, l'elemento passacavi, la presa a muro, il cavo 1061, i derivatori ad "Y", i cavetti di permutazione, i cavetti d'utente.

Il *wiring block* è l'elemento di terminazione su cui vengono attestati i cavi UTP. Su di esso si possono attestare fino a 100 coppie, in quanto è composto da 4 strisce telefoniche da 25 coppie cadauna. Due wiring block su cui sono attestati i cavi entranti su uno e quelli uscenti sull'altro, formano un permutatore.

Il *connecting block* è un blocchetto che va inserito in una delle strisce del wiring block e serve per la terminazione meccanica dei conduttori. Esso può essere, a seconda del modello, a 3, 4 o 5 coppie; lo sfruttamento completo di un wiring block si ha soltanto quando si utilizzano i connecting block da 5 coppie. Nel caso di cablaggio strutturato standard bisogna utilizzare i blocchetti da 4 coppie e quindi la potenzialità del blocco di terminazione si riduce a 96 coppie.

L'elemento passacavi può essere plastico, quando è interposto tra due wiring block, oppure metallico, quando è interposto tra due file di terminazioni. Esso serve ad organizzare la disposizione dei cavi.

La presa a muro, o placchetta, è disponibile in due versioni, con una o due prese RJ45. A sua volta, la placchetta con due prese è disponibile in una versione avente l'identificazione "Voice/Data" ed una avente l'identificazione "Line1/Line2".

Il cavo utilizzato è il 1061 dell'AT&T, che è di categoria 5 ed è non schermato.

I cavetti di permutazione utilizzati nell'armadio (di piano, di edificio o comprensorio) possono essere a 1, 2, 3 o 4 coppie; essi sono anche realizzabili in campo tramite l'utilizzo di attrezzature adeguate. Per i cablaggi ad alte prestazioni si usano esclusivamente cavetti precablati da 4 coppie di categoria 5.

I cavetti d'utente possono adattare le varie tipologie di connettori e cavi e possono contenere dei balun per adattare impedenze diverse.

La figura 4.43 mostra un esempio di cablaggio PDS.

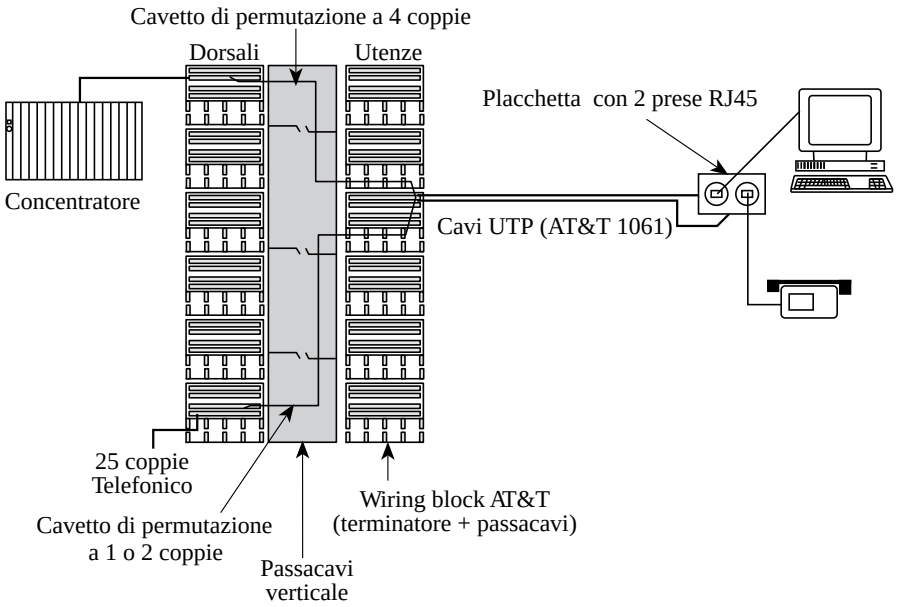


Fig. 4.43 - Esempio di cablaggio AT&T PDS.

4.10.5 Il sistema Trucco/SCP

Il sistema Trucco SCP (Sistema di Connessione Polivalente) è basato sulla permutazione telefonica; esso è costituito dai seguenti elementi principali: il modulo di permutazione, i telai di distribuzione, la presa a muro, i cavetti di permutazione, i cavetti d'utente.

Il modulo di permutazione è l'elemento di terminazione su cui vengono attestati i cavi UTP o FTP; su di esso si possono attestare fino a 8 coppie. Tale modularità permette un'associazione diretta tra il permutatore e la placchetta utente equipaggiata con due prese RJ45. Il modulo di permutazione è disponibile in cinque diverse colorazioni:

- il colore blu è utilizzato per la connessione del cavo utente;
- il colore verde è utilizzato per i cavi della dorsale telefonica;
- il colore giallo è utilizzato per i cavi della dorsale dati;
- il colore rosso è utilizzato per i cavi della dorsale dei segnali video;
- il colore arancio è utilizzato per la gestione tecnica (ad esempio: allarmi, sensori, lettori di badge).

I telai sono il supporto fisico per i moduli di permutazione e sono costituiti da un profilato d'acciaio ad "U" che fa anche funzione di passacavi posteriore.

La placchetta utente è basata sul passo 503 Ticino ed è corredata di due prese RJ45 di categoria 5.

I cavetti di permutazione sono preintestati e rispondono alle specifiche di categoria 5, sono disponibili in varie lunghezze e possono avere due modularità: a 2 coppie oppure a 4 coppie. La permutazione telefonica viene effettuata con la classica trecciola (doppino non schermato senza guaina) usata in telefonia.

I cavetti d'utente possono adattare le varie tipologie di connettori e cavi e possono contenere dei balun per adattare impedenze diverse.

La figura 4.44 mostra un esempio di cablaggio SCP.

4.10.6 Il sistema Krone

Il sistema Krone-LINK viene fornito sia in versione per cavi schermati (FTP o S-UTP) che per cavi UTP. I componenti passivi sono conformi alle specifiche di categoria 5.

La Krone è stata la prima industria ad introdurre un sistema a connessione rapida (LSA) per applicazioni telefoniche, in sostituzione dei contatti a saldare o a vite. Negli anni '80 La Krone ha brevettato il sistema a connessione rapida con

contatto inclinato a 45° rispetto al filo: inserendo il filo nel contatto, mediante l'apposito attrezzo di applicazione, due lamelle si deformano elasticamente e si torcono, penetrando nell'isolante e garantendo un contatto elettrico a tenuta di gas. Inoltre, la particolare caratteristica del contatto a 45° conferisce al sistema, oltre che bassissimi valori di resistenza di contatto (valore tipico 1 mΩ), anche un'elevata flessibilità: sullo stesso contatto possono essere attestati sia fili a conduttore pieno che a trecciola, con diametri da 0.4 mm a 0.8 mm.

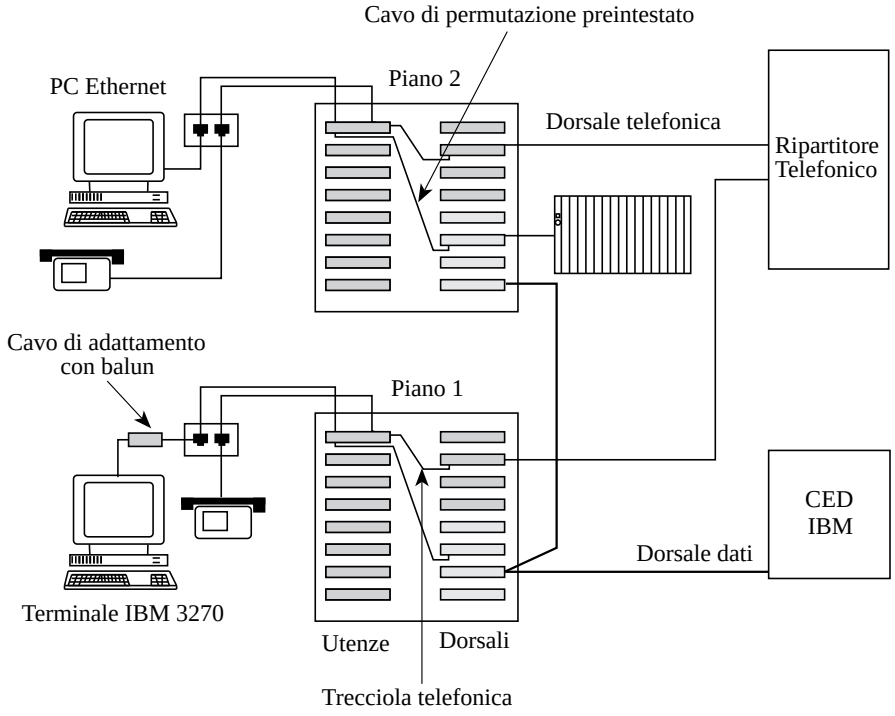


Fig. 4.44 - Esempio di cablaggio Trucco SCP.

La Krone fornisce due tipi di sistemi per il cablaggio integrato:

- uno di derivazione telefonica, basato sull'impiego di moduli di connessione a 8 o 10 coppie;
- uno, denominato RJ-HLN, basato su connettore di tipo RJ45 per la rete dati e RJ11 per la fonia, montati sia su pannelli modulari che nelle prese d'utente (figura 4.45).

I moduli RJ-KLN per le prese d'utente sono provvisti di protezione per salvaguardare i contatti dagli agenti atmosferici quando non utilizzati.

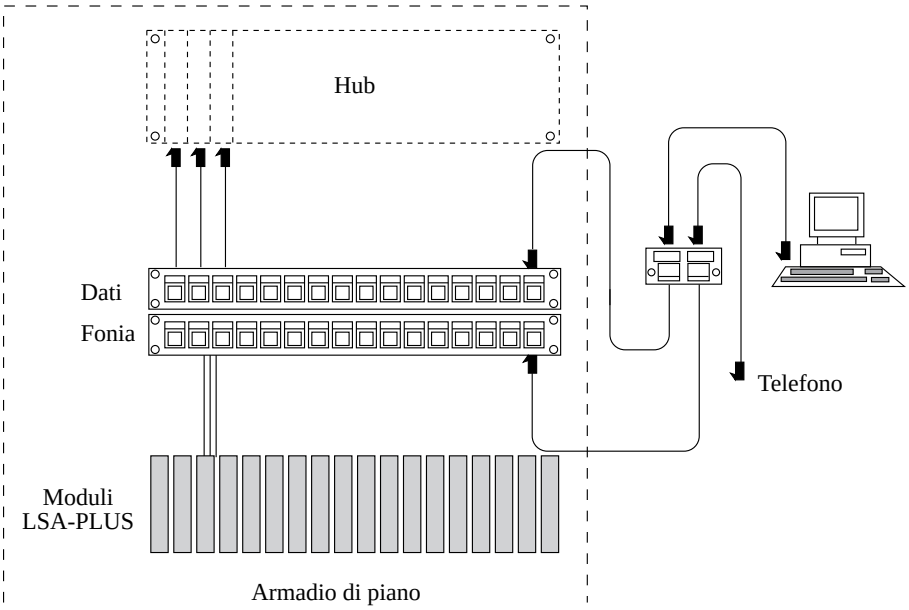


Fig. 4.45 - Il sistema RJ-KLN della Krone.

BIBLIOGRAFIA

[1] EIA/TIA-568, Commercial Building Telecommunications Wiring Standard (ANSI/EIA/TIA-568-91), July 1991.

[2] EIA/TIA-569, Commercial Building Standard for Telecommunications Pathways and Spaces (ANSI/EIA/TIA-569-90), October 1990.

[3] EIA/TIA-570, Residential and Light Commercial Building Telecommunications Wiring Standard (ANSI/EIA/TIA-570-91), June 1991.

[4] TIA/EIA-607, Commercial Buildinng Grounding and bonding Requirements for Telecommunications (ANSI/TIA/EIA-607-94), August 1994.

[5] TSB-36, Additional Cable Specifications for Unshielded Twisted Pair Cables, November 1991 (used in conjunction with EIA/TIA wiring standard).

[6] TSB-40, Additional Transmission Specification for Unshielded Twisted-Pair Connecting hardware, August 1992 (used in conjunction with EIA/TIA wiring standard and TSB36 above).

[7] DRAFT INTERNATIONAL STANDARD ISO/IEC 11801, Information Tecnology - Generic cabling for customer premise cabling.

[8] Standard Proposal No. 2840-A, Proposed Revision of EIA/TIA-568, Commercial Building Telecommunications Wiring Standard , July 13, 1994.

[9] Transmission Performance Specification for Field Testing of Unshielded Twisted-Pair Cabling System, DRAFT 11, March 21, 1995. Prepared by: ANSI/EIA/TIA PN-3287 Task Group on UTP Link Performance..

[10] IBMCentro di competenza Telecomunicazioni, "Reti Locali IBM: Sistema di cablaggio IBM", Codice documento GA13-1536-01, Roma (Italia), Set[8] AT&T Network System, "Systimax Premise Distribution System: Component Guide", Codice documento No. 555-400-603, dicembre 1990.

[11] Digital, "The DECconnect Communications System Handbook", Digital.

5

LE LAN E IL MODELLO DI RIFERIMENTO IEEE 802

La fine degli anni '70 vede la comparsa sul mercato statunitense delle LAN. Si tratta di reti di calcolatori che si propongono come scopo una soluzione più idonea al problema dell'interconnessione di sistemi su base locale di quanto non fossero le soluzioni progettate per le reti geografiche (WAN). Esse si basano sull'ipotesi che in ambito locale siano disponibili dei canali trasmissivi ad alta velocità, basso costo e non vincolati dalla conformità agli standard CCITT.

Una definizione che identifica gli aspetti peculiari delle LAN è la seguente:

5.1 DEFINIZIONE

> *Una LAN è un sistema di comunicazione che permette ad apparecchiature indipendenti di comunicare tra di loro, entro un'area delimitata, utilizzando un canale fisico a velocità elevata e con basso tasso d'errore.*

5.1.1 Apparecchiature indipendenti

Le reti geografiche costruite alla fine degli anni '70 erano quasi sempre basate sul concetto di master-slave. Il mainframe, o in generale l'elaboratore centrale, era il master della comunicazione, e i terminali, o le stazioni, gli slave. Tutti i sistemi connessi alla LAN diventano invece paritetici, cioè della stessa importanza. La "risorsa LAN" viene equamente ripartita tra tutti i sistemi ad essa connessi. Non conta la dimensione: per una LAN un mainframe è importante come un PC; non conta la

funzionalità: per una LAN un server è importante come un client. Inoltre, il funzionamento della LAN non dipende da alcun sistema in particolare. Essa continua a mantenere inalterate le sue funzionalità anche in presenza di guasti delle stazioni o dei mainframe, oppure nel caso in cui questi vengano collegati o scollegati.

5.1.2 Area delimitata

Le LAN non sottostanno agli standard CCITT, considerati troppo restrittivi, e quindi non possono prevedere l'attraversamento di suolo pubblico. Quindi il progetto delle LAN tiene conto che esse possono coprire solo un'area delimitata, cioè essere adibite ad uso esclusivo di una determinata persona o ente e posate all'interno di uno o più fondi contigui o collegati da opere aventi carattere permanente in conformità alle norme CEI 103-1 Ed. 1987.

5.1.3 Un canale fisico a velocità elevata

L'idea di usare un solo canale fisico di trasmissione per realizzare una LAN può a prima vista sembrare restrittiva, ma così non è. Quando le LAN fecero la loro comparsa sul mercato, spinte dai costruttori di calcolatori, i costruttori di sistemi di telecomunicazione cercarono di ostacolarle, proponendo come alternativa i PABX digitali. Questi sono dei centralini privati numerici in grado di commutare un grande numero di circuiti digitali a 64 Kb/s (velocità standard per un canale telefonico numerico). Fu un clamoroso fallimento e la diffusione delle LAN crebbe sempre più velocemente.

La causa di tale fallimento è da ricercarsi nella modalità operativa dell'utente di LAN. Egli infatti, contrariamente a quanto si potrebbe pensare, per la maggior parte del tempo non utilizza la rete. Quando però la utilizza, chiede alla rete di avere prestazioni altissime. Tale modalità di utilizzo viene detta "a burst". Questo mal si accorda con il modello del PABX numerico che alloca permanentemente a ciascun utente 64 Kb/s che sono inutilizzati per la maggior parte del tempo e di prestazioni troppo limitate quando l'utente decide di utilizzare la rete.

Il successo delle LAN è proprio da ricercarsi nell'aver compreso quanto sopra, ed effettuato la scelta progettuale rappresentata in figura 5.1.

Le LAN hanno quindi sempre un solo canale trasmissivo ad alta velocità condiviso nel tempo da tutti i sistemi collegati. Quando un sistema trasmette diventa proprietario temporaneamente (per la durata di uno o pochi pacchetti) dell'intera

capacità trasmissiva della rete. La trasmissione è sempre di tipo broadcast: un sistema trasmette e tutti gli altri ricevono. Tale organizzazione ha enormi vantaggi, ma impone anche alcune complicazioni: è necessaria la presenza di indirizzi per stabilire chi sono il reale destinatario e il mittente della trasmissione e occorre arbitrare l'accesso all'unico mezzo trasmissivo tra tutti i sistemi che hanno necessità di trasmettere.

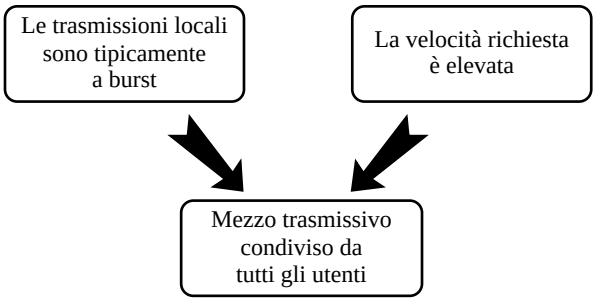

Le trasmissioni locali sono tipicamente a burst
La velocità richiesta è elevata
Mezzo trasmissivo condiviso da tutti gli utenti

Fig. 5.1 - La scelta progettuale delle LAN.

5.1.4 Basso tasso di errore

L'unico canale trasmissivo presente deve anche essere caratterizzato da un basso tasso di errore. Questo è ottenibile abbastanza facilmente in un'area delimitata usando mezzi trasmissivi di buona qualità, come discusso nei capitoli 3 e 4. L'effetto ottenuto è quello che le LAN, essendo intrinsecamente affidabili, non hanno la necessità di correggere gli errori a livello 2 OSI e quindi normalmente utilizzano protocolli di livello 2 connectionless ad alte prestazioni.

5.2 PROTOCOLLI E CABLAGGI

Il progetto iniziale delle LAN affronta sia problematiche relative ai protocolli di livello 2 sia problematiche relative al cablaggio delle LAN stesse. Una visione più moderna tende invece a separare i due problemi (figura 5.2).

Il problema del cablaggio strutturato degli edifici è già stato affrontato nel precedente capitolo 4. Ciò che occorre garantire è che le LAN siano in grado di usufruire dei mezzi trasmissivi accettati nello standard EIA/TIA 568. A tal scopo negli anni '90 tutte le LAN sono state modificate per soddisfare tale requisito.

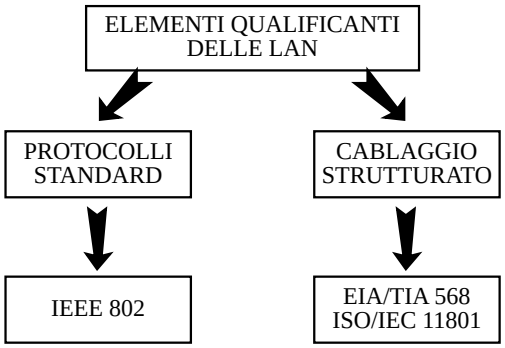


Fig. 5.2 - Protocolli e cablaggi.

5.3 ATTRIBUTI DI UNA LAN

Gli attributi che deve possedere una LAN sono quelli classici delle reti di calcolatori e cioè:

- *affidabilità*: oggi la tecnologia delle LAN è assolutamente consolidata e consente di ottenere affidabilità elevatissime, tali da permettere a molti costruttori di produrre schede di rete locale con garanzia illimitata;
- *flessibilità*: oggi le LAN sono utilizzate per applicazioni molto disparate, dalle LAN di soli PC all'integrazione PC-mainframe, fungendo da supporto unificato per più architetture di rete, tra loro incompatibili ai livelli superiori del modello OSI;
- *modularità*: le LAN possono essere realizzate utilizzando componenti di molti costruttori diversi, perfettamente intercambiabili;
- *espandibilità*: le LAN sono strutture appositamente concepite per fornire una crescita graduale nel tempo, secondo le esigenze dell'utente;
- *gestibilità:* la maggior parte dei componenti delle LAN prodotti negli ultimi anni sono concepiti per essere gestiti mediante accessi remoti utilizzando il protocollo SNMP (*Simple Network Management Protocol*), che è un protocollo applicativo basato su UDP/IP (si veda il paragrafo 16.12.9).

Affinché queste ed altre proprietà vengano soddisfatte è comunque indispensabile un accurato progetto a priori che tenga conto delle esigenze attuali dell'utilizzatore e delle possibili evoluzioni.

Le proprietà precedentemente elencate, unite all'*economicità*, sono state elemento chiave per la diffusione delle LAN e delle reti di calcolatori. Il soddisfacimento di

tali proprietà ha permesso di realizzare sistemi distribuiti concorrenziali con i mainframe non solo dal punto di vista economico, ma anche da quelli dell'affidabilità e delle prestazioni.

5.4 IL PROGETTO IEEE 802

Quando le prime LAN cominciarono a diffondersi (ARC, Ethernet, Token Ring, ecc.), l'IEEE decise di costituire sei comitati per studiare il problema della standardizzazione delle LAN e delle MAN, complessivamente raccolti nel progetto IEEE 802. Tali comitati sono:

- 802.1 Overview, Architecture, Bridging and Management;
- 802.2 Logical Link Control;
- 802.3 CSMA/CD (*Carrier Sense, Multiple Access with Collision Detection*);
- 802.4 Token Bus;
- 802.5 Token Ring;
- 802.6 Metropolitan Area Networks - DQDB (Distributed Queue, Dual Bus).

La struttura generale del progetto IEEE 802 è riportata in figura 5.3.

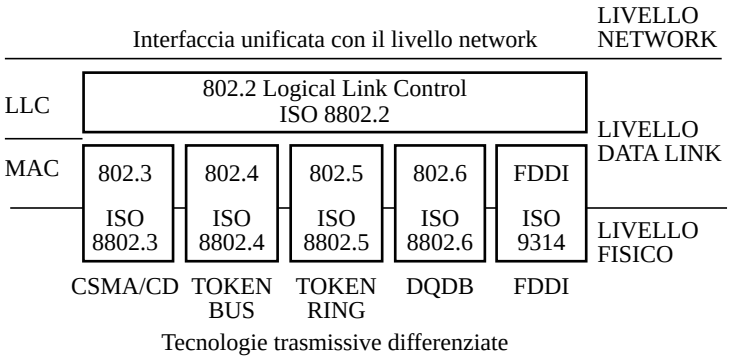


Fig. 5.3 - Il progetto IEEE 802.

A tali comitati in seguito se ne sono aggiunti altri tra cui:

- 802.3u 100BaseT;
- 802.7 Broadband technical advisory group;

- 802.8 Fiber-optic technical advisory group;
- 802.9 Integrated data and voice networks;
- 802.10 Network security;
- 802.11 Wireless network;
- 802.12 100VG AnyLAN;
- 802.14 Cable-TV based broadband communication network.

Il lavoro di tali comitati si svolse in armonia con il modello di riferimento OSI, e la relazione esistente tra il progetto OSI, il progetto IEEE 802 e lo standard EIA/TIA 568 è già stata evidenziata nel capitolo 2 (figura 2.12).

5.5 IEEE 802.1 HIGHER LAYER AND MANAGEMENT

È lo standard contenente le specifiche generali del progetto 802; esso è composto da molte parti, tra cui:

- *802.1 Part A* (Overview and Architecture);
- *802.1 Part B* (Addressing Internetworking and Network Management);
- *802.1 Part D* (MAC Bridges).

I concetti descritti dalle parti A e B sono stati già in parte introdotti e verrano ulteriormente dettagliati nel seguito di questo capitolo, mentre per quanto concerne 802.1-D esso verrà descritto approfonditamente nel capitolo 10.

IEEE 802 introduce l'idea che le LAN e le MAN devono fornire un'interfaccia unificata verso il livello Network (livello rete), pur utilizzando tecnologie trasmissive differenziate. Per ottenere tale risultato, il progetto IEEE 802 suddivide il livello Data Link in due sottolivelli:

- LLC (*Logical Link Control*);
- MAC (*Media Access Control*).

Il sottolivello LLC è comune a tutte le LAN, mentre il MAC è peculiare di ciascuna LAN, così come il livello fisico al quale è strettamente associato. Il sottolivello LLC è l'interfaccia unificata verso il livello Network ed è descritto nell'apposito standard IEEE 802.2, mentre i vari MAC sono descritti negli standard specifici di ogni rete locale (ad esempio il MAC CSMA/CD è descritto nello standard IEEE 802.3).

Nel seguito, per facilità di lettura, si parlerà solo di reti locali (LAN), ma quanto detto vale ovviamente anche per le reti metropolitane (MAN), comprese anch'esse nel progetto IEEE 802.

5.6 MAC

Il sottolivello MAC è specifico di ogni LAN e risolve il problema della condivisione del mezzo trasmissivo. Esistono vari tipi di MAC, basati su principi diversi, quali la contesa, il token, la prenotazione e il round-robin. Il MAC è indispensabile in quanto a livello 2 (Data Link) le LAN implementano sempre una sottorete trasmissiva di tipo broadcast in cui ogni sistema riceve tutti i frame inviati dagli altri.

Trasmettere in broadcast, cioè far condividere un unico canale trasmissivo a tutti i sistemi, implica la soluzione di due problemi:

- in trasmissione, verificare che il canale sia libero prima di trasmettere e risolvere eventuali conflitti di più sistemi che vogliano utilizzare contemporaneamente il canale;
- in ricezione, determinare a quali sistemi è effettivamente destinato il messaggio e quale sistema lo ha generato.

La soluzione del primo problema è data dai vari algoritmi di MAC che, per poter soddisfare il requisito 5.1.1 "apparecchiature indipendenti", devono essere algoritmi distribuiti su vari sistemi e non necessitare di un sistema master.

La soluzione del secondo problema implica la presenza di indirizzi a livello MAC (quindi nella MAC-PDU) che trasformino trasmissioni broadcast in:

- tramissioni punto-punto, se l'indirizzo di destinazione indica un singolo sistema;
- trasmissioni punto-gruppo, se l'indirizzo di destinazione indica un gruppo di sistemi;
- trasmissioni effettivamente broadcast, se l'indirizzo di destinazione indica tutti i sistemi.

Il MAC deve anche tener conto della topologia della LAN, che implica leggere variazioni sulle possibili modalità di realizzazione del broadcast: con topologie a bus, è un broadcast a livello fisico (elettrico), mentre con topologie utilizzanti canali punto-punto, quali l'anello, è un broadcast di tipo logico.

Le reti locali hanno canali sufficientemente affidabili, quindi non è in genere necessario effettuare correzione degli errori. Se ciò fosse richiesto, sarebbe il sottolivello LLC ad occuparsene essendo il MAC sempre connectionless.

I seguenti sottoparagrafi passano in rassegna brevemente i principali MAC, alcuni dei quali verranno descritti in dettaglio nei seguenti capitoli loro dedicati.

La tabella 5.1 riporta alcune date importanti per i tre principali standard.

LAN	Progetto Iniziale	Primo Standard	Prodotti Standard	Ampia Diffusione
802.3	1973	1980	1983	1985
802.5	1976	1982	1985	1987
FDDI	1981	1983	1989	1992

Tab. 5.1 - Date principali.

5.6.1 IEEE 802.3 (*CSMA/CD*)

IEEE 802.3 è l'evoluzione della rete Ethernet proposta da Digital, Intel e Xerox (DIX). Utilizza un MAC di tipo CSMA/CD (*Carrier Sense Multiple Access - Collision Detection*) in cui l'arbitraggio del canale trasmissivo avviene tramite un meccanismo di contesa non deterministico, che non garantisce un tempo di attesa limitato superiormente. IEEE 802.3 prevede una topologia logica a bus, con cablaggio a bus o a stella. La velocità trasmissiva è di 10 Mb/s e il throughput massimo di circa 4 Mb/s.

5.6.2 IEEE 802.4 (*Token Bus*)

IEEE 802.4 è uno standard di rete locale concepito appositamente per applicazioni di automazione di fabbrica, nell'ambito del progetto MAP (*Manufacturing Automation Protocol*). IEEE 802.4 ha una topologia logica e fisica a bus, ma l'arbitraggio del canale trasmissivo avviene tramite un token e quindi il protocollo è deterministico, con tempo di attesa limitato superiormente. La velocità trasmissiva è di 10 Mb/s e il throughput massimo di 8 Mb/s.

5.6.3 IEEE 802.5 (*Token Ring*)

IEEE 802.5 è l'evoluzione della rete locale Token Ring proposta da IBM in alternativa ad Ethernet. Lo standard prevede una topologia ad anello, con cablaggio stellare o a doppio anello. L'arbitraggio del canale trasmissivo avviene tramite token e quindi il protocollo è deterministico, con tempo di attesa limitato superiormente. La velocità trasmissiva è di 4 o 16 Mb/s e il throughput massimo di 3 o 12 Mb/s.

5.6.4 IEEE 802.6 (*DQDB*)

IEEE 802.6 è lo standard per reti metropolitane MAN, approvato anche in sede di CCITT. Utilizza una topologia logica a doppio bus, con cablaggio a doppio bus o a doppio anello. L'arbitraggio del canale trasmissivo avviene tramite prenotazioni gestite dall'algoritmo DQDB (*Distributed Queue Dual Bus*) e la tipologia del protocollo risulta deterministica. La velocità trasmissiva varia da 34Mb/s a 140 Mb/s con throughput massimi pari a circa l'80% della velocità trasmissiva.

5.6.5 FDDI

FDDI (*Fiber Distributed Data Interface*) è una rete locale ad alte prestazioni inserita nel progetto IEEE 802, ma standardizzata dall'ISO con la sigla 9314. Lo standard prevede una topologia logica ad anello, con cablaggio stellare o a doppio anello. L'arbitraggio del canale trasmissivo avviene tramite token e quindi la tipologia del protocollo è deterministica, con tempo di attesa limitato superiormente. La velocità trasmissiva è di 100 Mb/s e il throughput massimo di 80 Mb/s. FDDI è il primo standard per reti locali concepito esplicitamente per operare su fibra ottica, anche se oggi se ne hanno anche realizzazioni su rame.

5.6.6 MAC PDU

Nelle reti locali, al livello 2 OSI, sono presenti due tipi di PDU corrispondenti ai due sottolivelli LLC e MAC. Il formato della LLC-PDU è comune a tutte le reti locali e verrà discusso nel paragrafo 5.7.2, mentre quello della MAC-PDU è peculiare di ogni singolo MAC. Tuttavia alcuni campi principali, rappresentati in figura 5.4, sono presenti in tutte le MAC-PDU. In particolare una MAC-PDU contiene due indirizzi (SAP), uno di mittente (MAC-SSAP) e uno di destinatario (MAC-DSAP), un campo INFO contenente la LLC-PDU (cioè il pacchetto di livello LLC) e una FCS (*Frame Control Sequence*) su 32 bit, cioè un codice a ridondanza ciclica (CRC) per l'identificazione di errori di trasmissione.

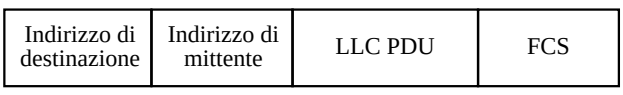


Fig. 5.4 - MAC-PDU.

5.6.7 Indirizzi MAC

Gli indirizzi MAC sono lunghi 6 byte, si scrivono per convenzione in esadecimale e sono univoci a livello mondiale. Essi sono scritti in una ROM dal costruttore della scheda di rete e possono essere eventualmente sostituiti via software da indirizzi scritti in un apposito buffer. Essi si compongono di due parti di 3 byte ciascuna:

- i 3 byte più significativi indicano il lotto di indirizzi assegnato al costruttore della scheda di rete locale o all'organizzazione che ha progettato una data architettura di rete; essi vengono detti OUI (Organization Unique Identifier);
- i 3 byte meno significativi sono una numerazione interna progressiva decisa dal costruttore stesso.

Ad esempio una scheda con indirizzo MAC 08-00-2B-3C-07-9A è una scheda prodotta dalla Digital Eq. Corp., in quanto il lotto 08-00-2B è l'OUI di tale ditta. Per una lista completa degli OUI si veda l'appendice A.

I primi due bit trasmessi sul canale hanno un'importanza particolare: il primo si chiama I/G (*Individual/Group*) ed indica se l'indirizzo è di un singolo sistema o di un gruppo di sistemi, il secondo U/L (*Universal/Local*) indica se l'indirizzo è stato assegnato ufficialmente o è stato deciso su base locale.

Vi sono purtroppo problemi di non standardizzazione nell'indirizzamento a livello MAC: in 802.3 e 802.4 il primo bit trasmesso sul filo è il meno significativo del primo byte, mentre in FDDI e 802.5 il primo bit trasmesso sul filo è il più significativo del primo byte. In figura 5.5 è illustrata tale disomogeneità.

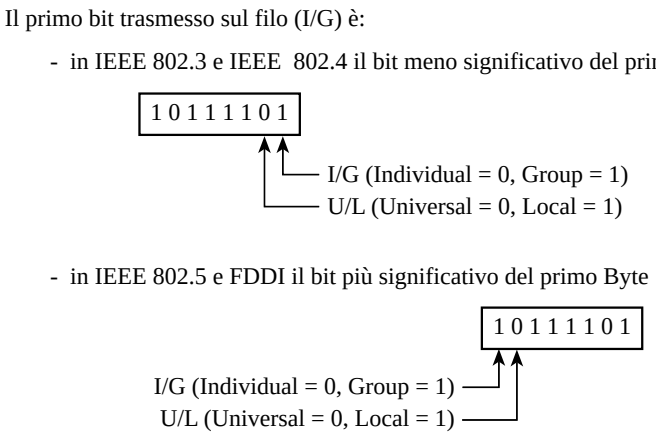

Il primo bit trasmesso sul filo (I/G) è:
- in IEEE 802.3 e IEEE 802.4 il bit meno significativo del primo Byte
1 0 1 1 1 1 0 1
I/G (Individual = 0, Group = 1)
U/L (Universal = 0, Local = 1)
- in IEEE 802.5 e FDDI il bit più significativo del primo Byte
1 0 1 1 1 1 0 1
I/G (Individual = 0, Group = 1)
U/L (Universal = 0, Local = 1)

Fig. 5.5 - Bit I/G e U/I.

Per superare i problemi introdotti da tale disomogeneità la IEEE ha introdotto il concetto che gli indirizzi devono sempre essere scritti e presentati all'esterno in un formato canonico (*canonical order*) indipendente dal tipo di rete locale. Il canonical order scelto è quello di 802.3 in cui i byte sono trasmessi nell'ordine di scrittura (da sinistra verso destra) e i bit all'interno dei byte vengono trasmessi dal meno significativo (destra) al più significativo (sinistra).

Le reti locali che usano una rappresentazione interna (*native order*) diversa, poiché trasmettono i bit da sinistra verso destra, devono farsi carico delle opportune conversioni. In tabella 5.2 sono riportati alcuni esempi di indirizzi MAC.

Canonical Order	Significato	Native Order 802.3 e 802.4	Native Order 802.5 e FDDI
08-00-2b-3c-56-fe	Individual Universal	08-00-2b-3c-56-fe	10-00-d4-3c-6a-7f
01-00-e5-7f-00-02	Multicast Universal	01-00-e5-7f-00-02	80-00-7a-fe-00-40
aa-00-04-00-65-27	Individual Local	aa-00-04-00-65-27	55-00-20-00-a6-e4
03-00-00-20-00-00	Multicast Local	03-00-00-20-00-00	c0-00-00-04-00-00
ff-ff-ff-ff-ff-ff	Broadcast	ff-ff-ff-ff-ff-ff	ff-ff-ff-ff-ff-ff

Tab. 5.2 - Esempi di indirizzi MAC.

Gli indirizzi MAC possono essere di tre tipi:

- *single*, se riferito ad un singolo sistema;
- *multicast*, se riferito ad un gruppo di sistemi;
- *broadcast*, se riferito a tutti i sistemi.

Il broadcast è un tipo particolare di multicast con codifica esadecimale FF-FF-FF-FF-FF-FF.

Quando una scheda di rete locale riceve un pacchetto, non lo passa automaticamente al livello superiore (LLC), ma effettua una serie di controlli. Per prima cosa verifica che il pacchetto sia integro (cioè abbia una FCS corretta) e di dimensioni ammesse. Quindi analizza l'indirizzo di destinazione (MAC-DSAP). Si possono porre tre casi:

- se il MAC-DSAP è broadcast, il pacchetto viene sempre passato al LLC;
- se il MAC-DSAP è single, il pacchetto viene passato al LLC solo se il MAC-DSAP è uguale all'indirizzo hardware della scheda o a quello caricato da software nell'apposito buffer;

- se il MAC-DSAP è multicast, si verifica se la ricezione di quel multicast è stata abilitata dal software di livello superiore, cioè se la scheda appartiene al gruppo indirizzato. Poiché non è noto a priori a quanti gruppi possa appartenere una scheda, si usano delle tecniche di hash per mantenere la lista dei gruppi abilitati.

Gli indirizzi di gruppo servono principalmente per scoprire quali altri sistemi sono collegati alla rete locale, quali servizi questi mettono a disposizione e le relazioni esistenti tra gli indirizzi MAC e gli indirizzi di livello 3. La trasmissione in multicast ha due diverse modalità d'impiego:

- *Solicitation*, un sistema che necessiti di accedere ad un dato servizio richiede, trasmettendo un pacchetto all'indirizzo di multicast di tale servizio, quali sistemi siano in grado di offrirlo. I sistemi che offrono il servizio rispondono alla richiesta;
- *Advertisement*, i sistemi che offrono un servizio trasmettono periodicamente tale informazione in multicast. Un esempio semplice è il messaggio di "Hello" con cui ogni sistema comunica periodicamente la sua esistenza e quindi la sua raggiungibilità sulla rete locale.

L'utilizzo di questi messaggi di multicast verrà descritto nel dettaglio nei capitoli sui protocolli di livello 3.

5.6.8 Relazioni tra L3, LLC e MAC

In figura 5.6 vediamo le relazioni tra le PDU di livello 3 (Network), le LLC-PDU e le MAC-PDU.

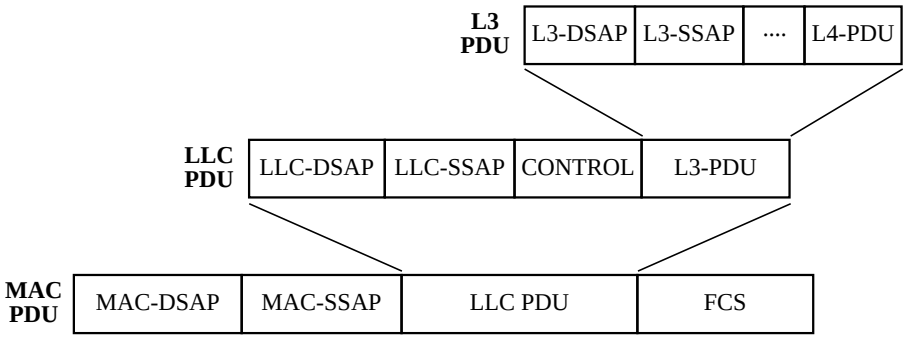


Fig. 5.6 - Relazione tra MAC-PDU e LLC-PDU.

Ogni interfaccia di rete locale è gestita da un suo livello MAC. Su tale livello MAC si appoggia un livello LLC. Il livello MAC è implementato nell'hardware della

scheda di rete locale, mentre il livello LLC è di solito realizzato in software. Ogni livello LLC può gestire un solo livello MAC: questo significa che un livello LLC non può avere funzionalità di "relaying" (non può inoltrare pacchetti) tra più MAC. Tale funzionalità di instradamento dei pacchetti è delegata al livello 3.

5.7 IEEE 802.2: LOGICAL LINK CONTROL

IEEE 802.2 è lo standard del sottolivello LLC. Esso definisce sia i servizi forniti dal livello LLC, sia il protocollo che li implementa.

5.7.1 Il protocollo LLC

LLC ha lo scopo di fornire un'interfaccia unificata con il livello network, il più simile possibile a quella delle reti geografiche. Per queste ultime l'OSI ha accettato come standard i protocolli della famiglia HDLC e quindi LLC è stato progettato come una variante di HDLC per le reti locali.

La differenza principale tra LLC e HDLC è che, mentre HDLC si appoggia direttamente sul livello fisico e quindi deve occuparsi della delimitazione delle trame e della trasparenza del campo dati, LLC si appoggia sul livello MAC cui viene demandata la soluzione di tali problemi. Quindi LLC è una versione semplificata di HDLC: non gestisce, ad esempio, la problematica del "bit stuffing", ma ha esattamente lo stesso formato del campo di controllo, per una descrizione del quale si rimanda al paragrafo 13.2.

LLC può operare sia come protocollo connesso che non connesso, anche se la modalità non connessa è quella più diffusa.

5.7.2 LLC-PDU

LLC ha una sua PDU (*LLC-PDU*), simile a quella di HDLC (figura 5.7). Si osservi che nel contesto dei protocolli per reti locali si suole usare il termine ottetto al posto di byte.

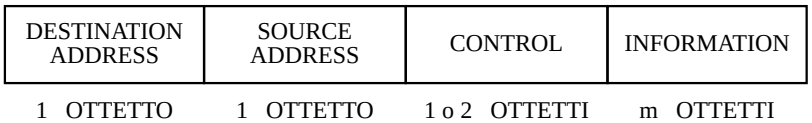


Fig. 5.7 - LLC-PDU.

In funzione dei valori assunti dal campo control, si distinguono tre tipi di PDU di cui il primo è il più importante:

- *Unnumbered PDU* (U-PDU). Si utilizzano per trasportare i dati di utente (nella modalità non connessa) per scopi di inizializzazione e per ragioni diagnostiche;
- *Information PDU* (I-PDU). Sono usate nella modalità connessa per trasportare i dati di utente;
- *Supervisory PDU* (S-PDU). Sono usate nella modalità connessa per trasportare le informazioni di controllo del protocollo.

Le U-PDU hanno un campo control di un byte, mentre le S-PDU e le I-PDU hanno un campo control di due byte.

In particolare si identificano tre sottotipi di U-PDU:

- *Unnumbered Information* (UI). Sono utilizzate per i dati di utente;
- *eXchange Identification* (XID). Sono usate per scambiare informazioni relativamente ai tipi di sevizi LLC disponibili;
- TEST. Sono usate per effettuare delle procedure di loopback test tra due sistemi.

Per un'analisi più approfondita dei vari tipi di LLC-PDU si veda il paragrafo 13.2.

5.7.3 Gli indirizzi LLC

Scopo di LLC è anche quello di fornire un supporto standard alla convivenza di più protocolli di livello superiore (ad esempio, DECnet, TCP/IP) sulla stessa LAN (figura 5.8). A tal fine LLC ha un suo SAP (*LLC-SAP*) che viene utilizzato per distinguere tra i protocolli di network che su di esso si appoggiano.

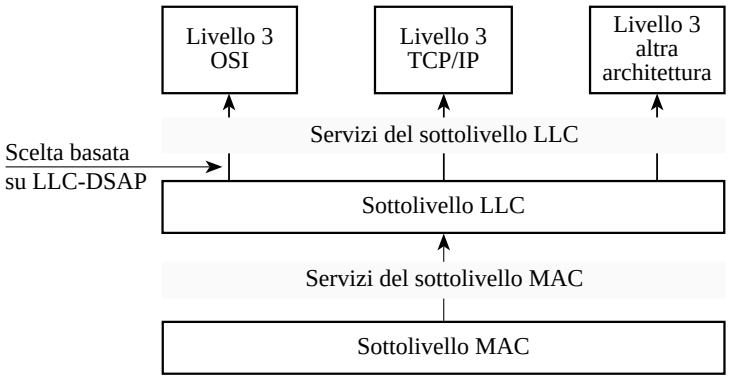


Fig. 5.8 - Supporto multiprotocollo offerto da LLC.

I SAP di LLC sono grandi un byte (figura 5.9) e i due bit meno significativi sono I/G (significato identico a quello di livello MAC) e U (attenzione: qui le codifiche sono scambiate: U = 0 indirizzo definito dall'utente, U = 1 indirizzo assegnato dall'IEEE).

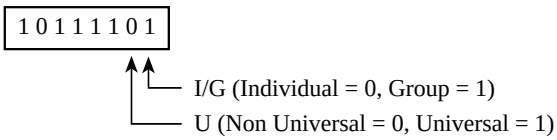


Fig. 5.9 - LLC SAP.

FF è l'indirizzo di broadcast e 00 indica il livello Data Link stesso. Rimangono quindi solo 63 codifiche utili ad indicare quale protocollo di livello superiore ha originato il pacchetto.

Visto che tale numero è insufficiente, ISO ha stabilito di attribuire una codifica ufficiale solo a quei protocolli approvati da un ente riconosciuto di standardizzazione. Ad esempio la codifica 0FEH indica il protocollo ISO 8473 (Internet Protocol connectionless di OSI) e la codifica 042H il protocollo IEEE 801.2D (Spanning Tree Configuration). Per un elenco esaustivo si veda l'appendice A.

5.7.4 Le SNAP-PDU

Quando i campi LLC-SAP assumono il valore 0AAH si ha un particolare pacchetto LLC, detto SNAP (*SubNetwork Access Protocol*), schematizzato in figura 5.10. I pacchetti SNAP servono per contenere le PDU di livello 3 dei protocolli proprietari e quindi non riconosciuti dall'ISO.

DSAP	SSAP	CONTROL	Protocol Identifier		INFORMATION
0AAH	0AAH	03H	000000H	0800H	L3-PDU
			OUI	Protocol Type	

Fig. 5.10 - LLC SNAP-PDU.

In tal caso il campo *Control* indica una U-PDU ed è seguito da un campo *Protocol Identifier* composto da due parti:

- i primi 3 byte contengono l'OUI dell'organizzazione che ha proposto il protocollo;
- i secondi 2 byte identificano il protocollo all'interno dell'organizzazione. Se i primi 3 byte sono a zero la codifica usata per questi 2 byte è quella del Protocol Type di Ethernet v.2.0, riportata in appendice A.

L'esempio di figura 5.10 indica un pacchetto con codifica Ethernet contenente dati TCP/IP, essendo 0800 la codifica per IP. Le codifiche Ethernet dei protocolli più comuni sono contenute nell'appendice A.

Un altro esempio è quello di un pacchetto con Protocol Identifier 08-00-2B-80-3C: si tratta di una SNAP-PDU usata da Digital (08-00-2B) per un protocollo proprietario utilizzato da applicativi di "name server".

Il livello LLC, quando riceve un pacchetto, analizza LLC-DSAP: se questo è diverso da 0AAH allora ha immediatamente il codice del protocollo di livello 3 a cui passare il pacchetto, altrimenti (è il caso di una SNAP-PDU) decide a quale livello 3 inoltrare il pacchetto in base al campo Protocol Identifier.

5.7.5 Servizi LLC

LLC offre al livello Network tre tipi di servizi:

- *Unacknowledged connectionless service* (LLC Type 1). In questa modalità il trasferimento dati è non connesso senza conferma. È la modalità preferita da molte architetture di rete proprietarie tra cui DECnet e TCP/IP;
- *Connection oriented service* (LLC Type 2). Questa modalità crea dei circuiti virtuali tra mittenti e destinatari prima di effettuare la trasmissione. È una modalità connessa, molto spesso adottata nelle architetture di rete IBM;
- *Semireliable service* (LLC Type 3). In questa modalità il trasferimento dati è non connesso, ma con conferma. È una modalità pensata per i protocolli da utilizzarsi in ambito di fabbrica.

I sistemi possono realizzare uno o più tipi di servizi LLC secondo la seguente classificazione:

- Classe I: realizza solo i servizi LLC tipo 1;
- Classe II: realizza i servizi LLC tipo 1 e 2;
- Classe III: realizza i servizi LLC tipo 1 e 3;
- Classe IV: realizza tutti i tre tipi di servizi LLC.

La grande diffusione di LLC tipo 1 è legata alle caratteristiche intrinseche delle LAN. Come visto nel paragrafo 5.14, uno dei requisiti fondamentali delle LAN è quello di avere un canale trasmissivo con un basso tasso di errore. È quindi il livello 1 (fisico) a garantire la qualità della trasmissione e non serve avere protocolli connessi a livello 2, come invece avviene nelle WAN, per le quali si utilizzano mezzi trasmissivi meno affidabili. Errori residui, sempre possibili, vengono corretti ad un livello superiore, quasi sempre a livello 4 (trasporto).

BIBLIOGRAFIA

[1] Cisco Systems, "Internetworking Technology Overview", Codice documento DOC-ITO13 78-1070-01, 1993.

[2] J. Martin, J. Leben, "DECnet Phase V: An OSI Implementation", Digital Press, Bedford MA (USA), 1992.

[3] R.P. Davidson, N.J. Muller, "Internetworking LANs: Operation, Design and Management", Artech House, London (UK), 1992.

[4] U. Black, "Computer Networks: Protocols, Standard and Interfaces", Prentice Hall, Englewood Cliffs N.J. (USA), 1987.

[5] F. Halsan, "Data Communications, Computer Networks and OSI", Addison Wesley Workinghan (UK), 1988.

[6] IEEE Std 802, "Overview and Architecture", Piscataway NJ (USA).

[7] ISO 8802-2 (ANSI/IEEE Std 802.2), "Logical Link Control".

[8] J. Reynolds, J. Postel, "RFC 1340: Assigned Number", July 1992.

[9] T. Pusatery, "RFC 1469: IP Multicast over Token-ring Local Area Network", June 1993.

[10] D. Katz, "RFC 1390: Transmission of IP and ARP over FDDI Networks", January 1993.

6

LA RETE ETHERNET E LO STANDARD IEEE 802.3

6.1 INTRODUZIONE

Nei primi anni '70 tre industrie di alta tecnologia formarono il consorzio DIX per lo sviluppo di una rete locale. DIX, dalle iniziali dei tre membri, Digital Equipment Corp., Intel Corp. e Xerox Corp., lavorò per circa 10 anni su una prima versione di Ethernet, la 1.0, operante a 10 Mb/s.

Nell'anno 1982 DIX pubblicò le specifiche di Ethernet versione 2.0: in quel momento nacque quella che sarebbe diventata la rete locale per antonomasia.

In parallelo il comitato americano IEEE iniziò lo sviluppo dello standard 802.3 che è basato su Ethernet, ma che differisce da questo per alcune caratteristiche logiche, riferite al livello Data Link, ed elettroniche (livello Fisico) riferite ai transceiver ed ai repeater. Nel 1985 lo standard IEEE 802.3 è stato adottato dal comitato tecnico 97 dell'ISO come DIS (*Draft International Standard*) ISO/DIS 8802.3 e nel 1989 approvato come standard ISO 8802.3.

Negli anni successivi il comitato IEEE ha lavorato per migliorare le caratteristiche e la flessibilità del livello fisico del 8802.3, aggiungendo l'uso di diversi mezzi trasmissivi; l'ultimo supplemento è stato pubblicato il 13 ottobre 1993.

I costi ridotti degli apparati e la grande facilità di progettare e realizzare reti di piccole dimensioni sono state le chiavi di successo di Ethernet e, sebbene ormai quasi tutti gli apparati in commercio siano conformi alle specifiche 802.3, essi vengono spesso identificati con il nome originale *Ethernet*.

Nei successivi sottoparagrafi tratteremo:

- il metodo di accesso CSMA/CD in quanto è comune sia ad Ethernet sia a 802.3 (si veda il paragrafo 6.2);
- le principali caratteristiche di Ethernet versione 2.0, in quanto è possibile

trovare in vecchie installazioni di rete apparati conformi a queste specifiche (si veda il paragrafo 6.3);

- le caratteristiche di 802.3 in modo approfondito ed i supplementi relativi ai diversi mezzi trasmissivi ammessi (si veda il paragrafo 6.4);
- le regole per configurare correttamente una LAN IEEE 802.3 (si vedano i paragrafi 6.5, 6.6 e 6.7);
- la convivenza dei due standard in reti locali miste (si veda il paragrafo 6.8).

6.2 METODO DI ACCESSO CSMA/CD

Le reti Ethernet e 802.3 sono nate con una topologia a bus basata su cavo coassiale, con velocità trasmissiva di 10Mb/s, e coinvolgono il livello 1 della pila OSI ed il sottolivello MAC del livello 2 (figura 6.1).

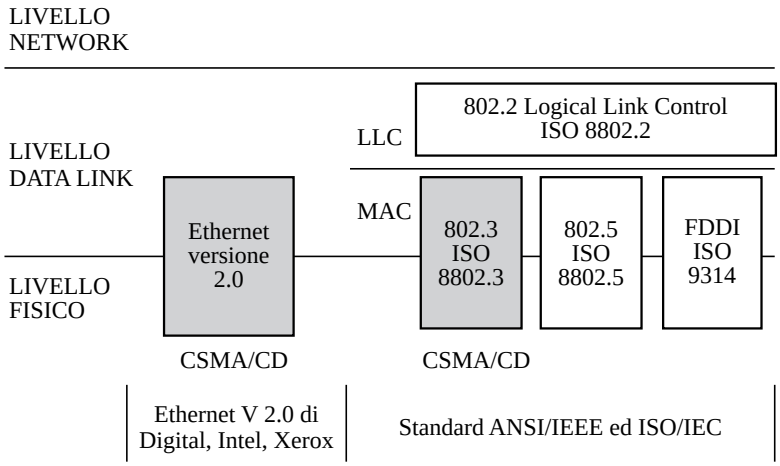


Fig. 6.1 - Relazioni tra i livelli OSI ed Ethernet e 802.3.

Il MAC (Media Access Control), cioè il metodo usato per arbitrare l'utilizzo del canale trasmissivo tra le stazioni della rete, è il CSMA/CD, identico in Ethernet e in 802.3. Esso è stato progettato per l'utilizzo del cavo coassiale come mezzo trasmissivo, ma è stato mantenuto inalterato anche in seguito all'introduzione di altri mezzi trasmissivi quali la fibra ottica ed il doppino. CSMA/CD significa Carrier Sense Multiple Access with Collision Detection e consiste in un protocollo

totalmente distribuito, senza stazioni master, per permettere alle stazioni di condividere l'utilizzo del mezzo trasmissivo comune. Poiché mediante il collegamento a bus i trasmettitori delle stazioni si trovano ad essere "in parallelo", è necessario evitare che più stazioni trasmettano contemporaneamente. Tuttavia, il protocollo non esclude che ciò possa comunque avvenire, e prevede un meccanismo di riconoscimento di tale evento da parte delle stazioni coinvolte in modo che possano ritentare la trasmissione in un tempo successivo.

Il protocollo opera in tre diverse fasi:

- *carrier sense* (rilevazione della trasmissione): ogni stazione che deve trasmettere ascolta il bus e decide di trasmettere solo se questo è libero (*listen before talking*);
- *multiple access*: nonostante il carrier sense è possibile che due stazioni, trovando il mezzo trasmissivo libero, decidano contemporaneamente di trasmettere; la probabilità di questo evento è aumentata dal fatto che il tempo di propagazione dei segnali sul cavo non è nullo, e quindi una stazione può credere che il mezzo sia ancora libero anche quando un'altra ha già iniziato la trasmissione;
- *collision detection*: se si verifica la sovrapposizione di due trasmissioni si ha una "collisione"; per rilevarla, ogni stazione, mentre trasmette un pacchetto, ascolta i segnali sul mezzo trasmissivo, confrontandoli con quelli da lei generati (*listen while talking*).

Le figure 6.2 e 6.3 illustrano una trasmissione senza collisioni ed una trasmissione con collisione. Occorre evidenziare che la collisione non è un errore trasmissivo, ma è banda impiegata per arbitrare il canale. La presenza di un numero limitato di collisioni su una rete locale di questo tipo non è quindi un sintomo di malfunzionamenti, ma è funzionale all'arbitraggio della rete stessa (si veda il paragrafo 6.2.3).

A seguito di un'avvenuta collisione si intraprendono le seguenti azioni:

- la stazione trasmittente sospende la trasmissione e trasmette una sequenza di *jamming* (interferenza trasmissiva) composta da 32 bit per 802.3 ed un numero di bit compreso tra 32 e 48 per Ethernet v.2.0; questa sequenza permette a tutte le stazioni di rilevare l'avvenuta collisione;
- le stazioni in ascolto, riconoscendo il frammento di collisione costituito dalla parte di pacchetto trasmessa più la sequenza di jamming, scartano i bit ricevuti;
- la stazione trasmittente ripete il tentativo di trasmissione dopo un tempo pseudo-casuale per un numero di volte non superiore a 16.

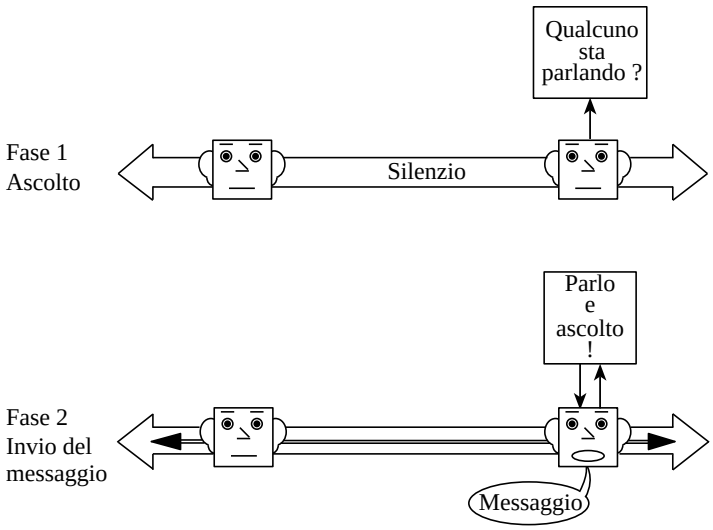


Fig. 6.2 - Trasmissione senza collisione.

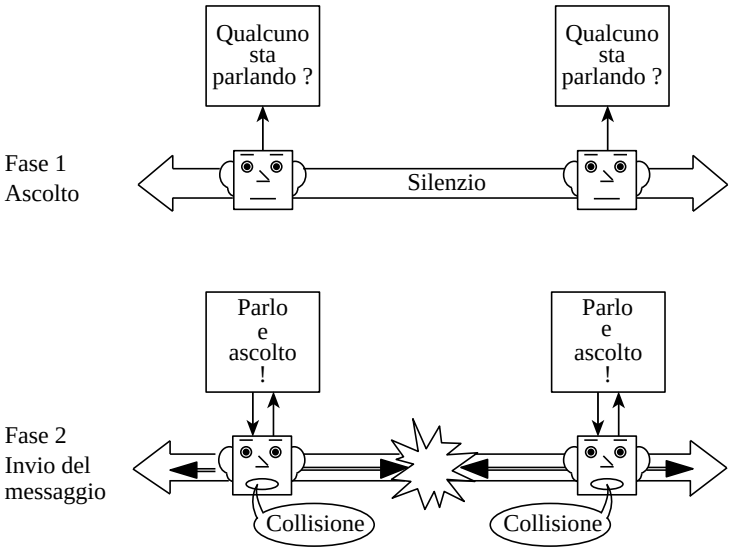


Fig. 6.3 - Trasmissione con collisione.

La schedulazione della ritrasmissione in base ad un tempo di attesa pseudo-casuale evita che dopo una collisione le stesse stazioni che l'hanno generata ritrasmettano contemporaneamente; il tempo di attesa è determinato da un algoritmo di back-off detto *truncated binary exponential backoff*. Il ritardo è un multiplo intero dello slot time (512 bit, cioè 51.2 μs) preso come tempo base, e all'*n*-esimo tentativo di ritrasmissione il numero di tempi base *r* da attendere è scelto casualmente nell'intervallo $0 \leq r < 2^k$, dove $k = \min(n,10)$.

6.2.1 Parametri del protocollo

Affinché le stazioni siano sempre in grado di rilevare le eventuali collisioni è necessario che siano rispettati alcuni vincoli tra i parametri di progetto della rete. In particolare, per garantire che la stazione trasmittente possa accorgersi della presenza di una qualsiasi collisione, è necessario che essa rimanga in trasmissione per un tempo sufficientemente lungo per permettere a tutte le possibili trasmissioni che generano collisione di propagarsi fino ad essa (si osservi che la collisione può essere rilevata soltanto durante la trasmissione, e non dopo).

È sufficiente analizzare il caso peggiore, cioè quello in cui due stazioni, A e B, sono alle estremità opposte di una rete di estensione massima. Si supponga che A debba trasmettere e trovi il mezzo libero. Si supponga che anche B debba trasmettere, e verifichi la disponibilità del mezzo un istante prima che il primo bit della trasmissione di A la raggiunga. Non appena B inizia a trasmettere rileva la collisione, e invia la sequenza di jamming. Ma affinché anche A si accorga della collisione, la sua trasmissione deve durare finché l'inizio della trasmissione di B non si è propagato fino a lei. Quindi una trasmissione deve durare almeno il tempo necessario ad un bit per propagarsi da un estremo all'altro (da A a B) e poi al contrario (da B ad A). Questo tempo prende il nome di *round trip delay*, ed è uno dei parametri di progetto delle reti CSMA/CD. Altri parametri sono la dimensione massima della rete, la velocità di trasmissione (in bit/s), il numero minimo di bit per ogni pacchetto, la distanza minima tra i pacchetti.

Nota la velocità di propagazione dei segnali sul cavo (circa 2/3 della velocità della luce nel vuoto) e decisa la velocità di trasmissione è possibile definire uno degli altri parametri e calcolare i rimanenti. In Ethernet la velocità di trasmissione è di 10 Mb/s, e la dimensione minima del pacchetto è fissata in 512 bit più 64 bit di preambolo per la sincronizzazione e di *start frame delimiter*; la durata della trasmissione di un pacchetto è quindi di almeno 57.6 μs, e questo è il massimo round trip delay ammissibile. La metà di tale tempo è il massimo tempo di propagazione di

un segnale da un estremo all'altro della rete, che, alla velocità di propagazione di circa $2 \cdot 10^8$ m/s, corrisponderebbe ad una estensione massima di oltre 5 Km. In pratica, però, l'attenuazione introdotta dai cavi non consente di realizzare una rete di tale estensione senza ripetitori. Essi, insieme ai vari elementi attivi e passivi di collegamento, introducono dei ritardi nella propagazione dei segnali. Tali ritardi impongono, per non superare il massimo round trip delay, una riduzione dell'estensione totale dei cavi. È anche necessario introdurre un certo margine di sicurezza nei parametri temporali per considerare le tolleranze dei componenti. Il calcolo accurato del round trip delay e le varie versioni delle regole di configurazione di Ethernet e di 802.3 basate su di esso saranno discussi nei paragrafi 6.6 e 6.7.

6.2.2 Caratteristiche funzionali

Il metodo di accesso CSMA/CD è responsabile delle seguenti operazioni:

- trasmissione dei pacchetti: durante questa fase il MAC accetta un pacchetto dal livello superiore e fornisce una stringa seriale di bit al livello fisico per la loro trasmissione sul mezzo fisico;
- ricezione dei pacchetti: durante questa fase il MAC riceve una stringa seriale di bit dal livello fisico e fornisce il pacchetto al livello superiore. Nel caso in cui il pacchetto non sia indirizzato alla stazione ricevente (singolo o multicast), né sia un pacchetto broadcast, viene scartato;
- trasmissione in modalità differita di un pacchetto, quando il canale è occupato;
- generazione del campo FCS per i pacchetti trasmessi;
- controllo del campo FCS in ricezione: il MAC verifica che non ci siano errori nel pacchetto ricevuto confrontando il valore contenuto nel campo FCS del pacchetto ricevuto con quello calcolato localmente. In caso di errori scarta il pacchetto senza richiederne la ritrasmissione: il MAC gestisce infatti sempre un protocollo non connesso;
- spaziatura dei pacchetti: il MAC garantisce che tra due pacchetti consecutivi intercorra un lasso di tempo minimo pari al parametro che viene identificato con i nomi di *Inter Frame Spacing* (IFS) o *Inter Packet Gap* (IPG). Questo tempo serve a delimitare la fine di un pacchetto e a separarlo da quello successivo;
- rilevazione delle collisioni: il MAC interrompe la trasmissione quando rileva una collisione;

- schedulazione delle ritrasmissioni: il MAC schedula la ritrasmissione a seguito di un'avvenuta collisione dopo il periodo di tempo calcolato tramite l'algoritmo di backoff;
- jamming: il MAC trasmette un messaggio di jamming a seguito della rilevazione di una collisione e dopo aver interrotto la trasmissione del pacchetto;
- verifica della lunghezza minima del pacchetto: il MAC scarta i pacchetti ricevuti che hanno una lunghezza inferiore al valore minimo ammesso (64 byte);
- generazione del preambolo: in trasmissione il MAC prepone un preambolo al pacchetto che deve essere trasmesso;
- rimozione del preambolo: in ricezione il MAC rimuove il preambolo.

6.2.3 Collision domain

In una singola rete CSMA/CD il mezzo trasmissivo è condiviso tra tutte le stazioni che se ne contendono l'utilizzo mediante il protocollo appena visto. Al crescere del numero di stazioni e/o del traffico aumenta la probabilità di collisioni e quindi diminuisce l'efficienza della rete. È possibile suddividere la rete in più sottoreti in modo che la contesa del mezzo avvenga soltanto tra le stazioni appartenenti ad una singola sottorete. Si dice che ciascuna sottorete rappresenta un singolo *collision domain*. Le stazioni separate da repeater fanno parte dello stesso collision domain, mentre fanno parte di collision domain diversi le stazioni separate da apparecchiature di rete che lavorano a livelli OSI superiori al Fisico (bridge, router o gateway) e che quindi sono in grado di decodificare gli indirizzi MAC e filtrare i pacchetti.

6.2.4 Prestazioni

La natura non deterministica del CSMA/CD rende complessa la valutazione delle prestazioni. I valori che si trovano in letteratura sono abbastanza diversi in funzione del fatto che l'autore sia un sostenitore o un detrattore del CSMA/CD.

È opinione degli autori che il CSMA/CD si sia sempre comportato in campo molto meglio di quanto previsto dai modelli teorici. Prova ne sia il fatto che è stato ampiamente usato anche in ambiti dove sono importanti le caratteristiche di tempo reale, quale quello di fabbrica.

È conservativo suggerire che CSMA/CD possa sopportare un carico medio del 30% (3 Mb/s come prestazione media effettiva) con picchi del 60% (6 Mb/s). È

però indubbiamente vero che bisogna anche considerare il numero di stazioni attive sulla LAN e la direzione dei flussi di traffico. A parità di traffico totale, se vi sono poche stazioni molto attive le prestazioni sono migliori di quando vi sono molte stazioni mediamente meno attive. Nel caso limite di due sole stazioni le prestazioni possono raggiungere il 90%.

Con un carico medio del 30% è stato osservato che il 50% dei pacchetti sono *initially deferred*, cioè nella fase di listen before talking trovano il mezzo trasmissivo occupato e, atteso che questo si liberi, vengono quindi trasmessi con successo al primo tentativo. Il 2-3% dei pacchetti hanno una *single collision*, cioè durante il primo tentativo di trasmissione entrano in collisione con un altro pacchetto e al secondo tentativo vengono trasmessi con successo. Infine qualche pacchetto su diecimila ha una *multiple collision*, cioè richiede più di due tentativi per essere trasmesso.

In una rete ben funzionante con un carico del 30% è altamente improbabile osservare un pacchetto che non può essere trasmesso perchè supera il limite di 16 tentativi.

6.3 ETHERNET VERSIONE 2.0

Lo standard Ethernet si colloca nei primi due livelli della pila OSI senza seguire gli standard IEEE 802 ed in particolare senza adottare il protocollo IEEE 802.2 LLC.

La differenza principale è nel diverso tipo di imbustamento, differenza che è importante comprendere in quanto molti protocolli di livello 3 usano questa metodologia di imbustamento invece di usare quella 802.3. L'utilizzo di imbustamento Ethernet è comune anche su hardware 802.3 in quanto è elevato il livello di interoperabilità e di convivenza tra i due standard.

In questo paragrafo vengono descritte le LAN Ethernet così come specificate nello standard v.2.0. La descrizione dell'utilizzo molto comune di imbustamento Ethernet su hardware 802.3 viene demandato al paragrafo 6.8.

Le figure 6.1 e 6.4 mostrano le relazioni tra Ethernet e i livelli di riferimento OSI.

6.3.1 Livello Fisico

Le principali caratteristiche relative al livello fisico sono:

- velocità trasmissiva 10 Mb/s;

- 2.8 km di distanza massima ammessa tra le due stazioni più distanti;
- 1024 stazioni al massimo in una LAN;
- cavo coassiale di tipo thick (tipo RG213, si veda in proposito il paragrafo 3.2.7) come unico mezzo trasmissivo ammesso;
- topologia a bus.

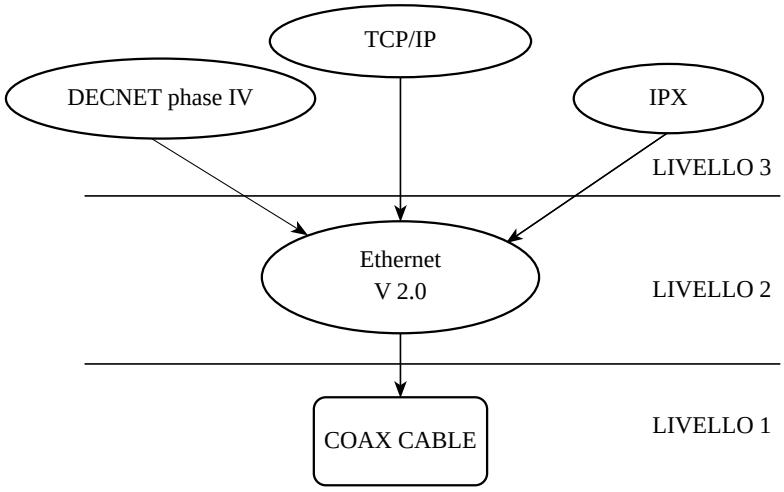


Fig. 6.4 - Relazione tra Ethernet v. 2.0 e i livelli OSI.

6.3.2 Livello Data Link

Le principali funzioni di Ethernet relative al livello Data Link sono quelle già descritte nel paragrafo 6.2. I parametri principali del livello Data Link sono riportati in tabella 6.1.

Il pacchetto Ethernet (figura 6.5) ha una lunghezza variabile compresa tra 64 e 1518 ottetti.

In testa al pacchetto c'è un preambolo di 7 ottetti (sequenza alternata di uni e di zeri) che serve alla stazione ricevente per sincronizzarsi sul clock di quella trasmittente; immediatamente dopo c'è un ottetto di *SFD* (*Start Frame Delimiter*, corrispondente alla sequenza di bit 11010101) che indica l'inizio del pacchetto.

Nel campo di *destination address* è contenuto l'indirizzo della stazione a cui è destinato il pacchetto, e nel campo di *source address* è contenuto l'indirizzo della stazione che ha generato il pacchetto.

Slot time	512 bit time (51.2 μs)	Tempo base di attesa prima di una ritrasmissione
Inter Packet Gap	9.6 μs	Distanza minima tra due pacchetti
Attempt limit	16	Massimo numero di tentativi di ritrasmissione
Backoff limit	10	Numero di tentativi oltre al quale non aumenta più la casualità del back-off
Jam size	da 32 a 48 bit	Lunghezza della sequenza di jam
Max frame size	1518 ottetti	Lunghezza massima del pacchetto
Min frame size	64 ottetti (512 bit)	Lunghezza minima del pacchetto
Address size	48 bit	Lunghezza indirizzi MAC

Tab. 6.1 - Ethernet: principali parametri.

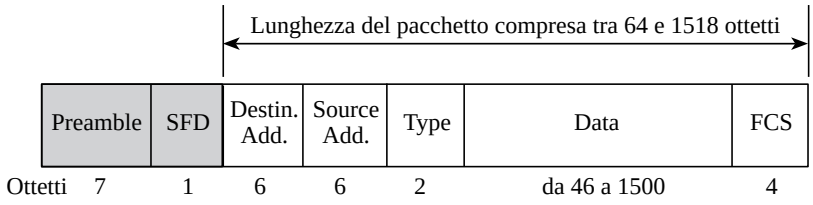


Fig. 6.5 - Formato del pacchetto Ethernet.

Nel campo *type* è contenuto il codice associato al protocollo di livello superiore che ha generato la PDU contenuta nel campo *data* (i valori possibili per tale campo sono riportati in appendice A, paragrafo A.2).

Il campo FCS (*Frame Check Sequence*) contiene il valore di CRC calcolato sulla base dei campi descritti precedentemente.

Si noti che non esiste un segnalatore di fine pacchetto: tale ruolo è assunto dall'Inter Packet Gap, la cui durata non può quindi scendere sotto il valore minimo fissato in 9.6 μs.

6.3.3 Cavo coassiale

Il cavo coassiale è l'unico mezzo trasmissivo ammesso per collegare le stazioni. Esso viene considerato "segmento" ("segmento coax"), mentre la fibra

ottica viene considerata solo come un mezzo per estendere la connessione tra due segmenti coax tramite l'uso di una coppia di half-repeater. Un segmento può essere costituito da un unico spezzone di cavo o da più spezzoni connessi con un giunto di tipo "N"; in quest'ultimo caso gli spezzoni devono avere una lunghezza definita in modo che, in una qualunque combinazione, la giunzione non capiti ad una distanza pari ad un multiplo dispari intero della lunghezza d'onda a 5 MHz. Per questa ragione sono state definite tre lunghezze di spezzoni: 23.4, 70.2 e 117 m.

Le caratteristiche minime richieste riguardanti il cavo coassiale sono le seguenti:

- impedenza 50 ± 2 Ω;
- velocità di propagazione minima 0.77 c, dove c è la velocità della luce;
- attenuazione massima del segmento (500 m) 8.5 dB misurata a 10 MHz e 6 dB misurata a 5 MHz.

6.3.4 Transceiver

Il transceiver è l'elemento che permette la trasmissione/ricezione dei pacchetti tra l'interfaccia (Ethernet controller) ed il mezzo trasmissivo (cavo coassiale). L'interfaccia è collegata al transceiver tramite un cavo transceiver (figura 6.6).

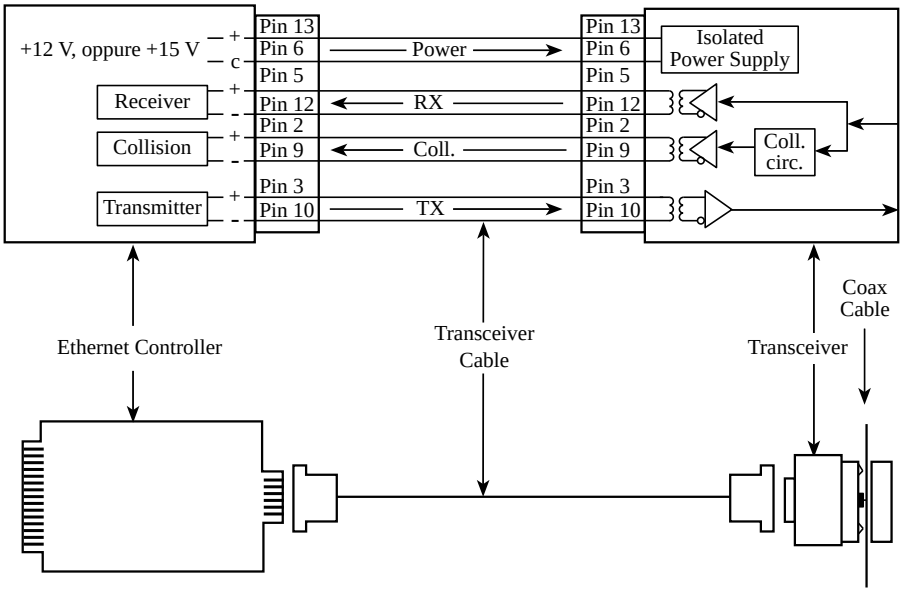


Fig. 6.6 - Connessioni tra interfaccia e transceiver.

Il transceiver è costituito principalmente da:

- due driver di cui:
  - uno trasmette all'interfaccia i dati ricevuti dal mezzo trasmissivo;
  - l'altro invia all'interfaccia un segnale di collisione nel caso in cui questa sia avvenuta; inoltre il driver di collisione invia all'interfaccia, alla fine di ogni trasmissione, un segnale chiamato *Collision Presence Test* (CPT o *Heartbeat*) il cui scopo è testare il circuito di collisione ed avvisare l'interfaccia del corretto funzionamento di tale circuito;
- un receiver che riceve i dati dall'interfaccia e li trasmette, tramite ulteriori circuiti, sul mezzo trasmissivo;
- un alimentatore (convertitore DC/DC) che riceve l'alimentazione dall'interfaccia e genera l'alimentazione per i circuiti elettronici interni al transceiver, senza creare continuità tra le masse elettriche.

Il transceiver si collega al cavo coassiale tramite un sistema di accoppiamento meccanico detto tap, che perfora il cavo tramite una punta dorata e va a toccare il conduttore centrale. Tale connessione, anche detta a vampiro, è mostrata in figura 6.7.

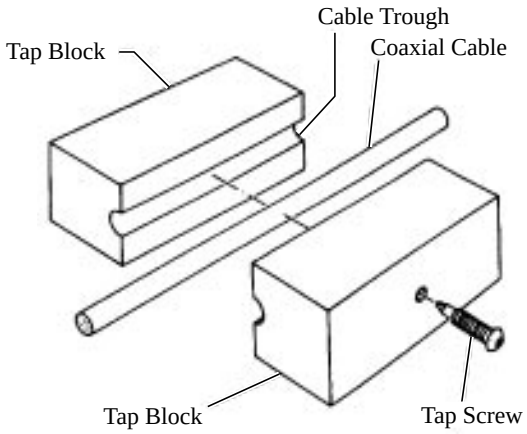


Fig. 6.7 - TAP connector (connessione a vampiro).

6.3.5 Interfaccia Ethernet

L'interfaccia Ethernet o Ethernet controller è il modulo d'interfaccia tra il bus interno della stazione ed il transceiver (figura 6.8).

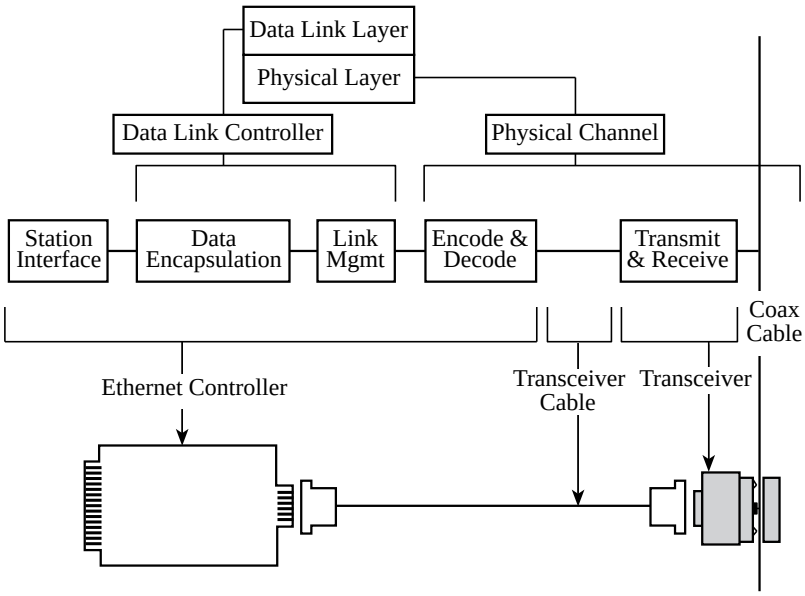


Fig. 6.8 - Funzioni logiche dell'interfaccia Ethernet.

L'interfaccia si occupa delle seguenti funzioni:

- incapsulamento e decapsulamento dei dati;
- link management;
- codifica e decodifica Manchester dei bit: per trasmettere il segnale di clock insieme ai dati, ad ogni bit viene applicata una codifica Manchester che garantisce almeno una transizione del segnale elettrico in ogni bit (si veda il paragrafo 3.1.2). Questo permette ad appositi circuiti del ricevitore di agganciare in fase il loro clock a quello del trasmettitore durante la ricezione del preambolo e quindi di effettuare una ricezione del pacchetto con la corretta temporizzazione.

6.3.6 Cavo transceiver

Il cavo transceiver, detto anche cavo drop o AUI, interconnette un transceiver ad un'interfaccia Ethernet o ad un ripetitore. Si tratta di un cavo schermato con connettori a 15 poli. La trasmissione dei segnali è bilanciata.

6.3.7 Repeater

Il repeater (ripetitore) serve ad estendere la lunghezza del canale trasmissivo e realizzare topologie ad albero. Viene definito ripetitore l'elemento attivo che interconnette due cavi coassiali. Esso richiede due transceiver per connettere i due segmenti. I transceiver possono essere connessi al ripetitore tramite due cavi transceiver.

Le funzioni principali di un ripetitore Ethernet v.2.0 sono le seguenti:

- ripete le stringhe di bit ricevuti su un segmento e le trasmette sugli altri segmenti con un'ampiezza di segnale appropriata;
- assicura che la simmetria dei segnali sia entro la tolleranza richiesta dalle specifiche del transceiver;
- decodifica, secondo il metodo Manchester, le stringhe seriali di bit ricevute su una porta e le ricodifica prima di ritrasmetterle sulle altre porte, ritemporizzando quindi tutti i bit da trasmettere (*reclock* dei bit o funzione di *retiming*);
- si occupa della gestione della collisione: se una collisione viene rilevata su una qualunque porta, il ripetitore la ritrasmette, presentando una serie di transizioni non ben specificate, su tutte le altre porte.

Le funzioni del ripetitore possono essere separate in due parti attive distinte che vengono interconnesse tramite una fibra ottica e che prendono il nome di half-repeater (mezzo ripetitore).Una coppia di half-repeater o ripetitori remoti serve ad interconnettere due segmenti coassiali tramite un link in fibra ottica.

A differenza del ripetitore 802.3, quello Ethernet non rigenera il preambolo, quindi "taglia" la parte del preambolo che impiega per sincronizzarsi. In tal modo il preambolo si accorcia ogni volta che attraversa un ripetitore e quindi bisogna porre un limite massimo al numero di ripetitori che un pacchetto può attraversare su una rete Ethernet più stringente di quando non avvenga nel caso 802.3.

6.3.8 Regole di configurazione

Le regole riguardanti il segmento coassiale sono:

- la lunghezza massima del segmento coassiale è di 500 m;
- la lunghezza massima di un cavo transceiver è di 50 m;
- la distanza minima tra due transceiver è di 2.5 m;
- il numero massimo di transceiver collegabili in un segmento è 100.

Le regole riguardanti il numero dei ripetitori sono:

- in un qualsiasi percorso tra due stazioni si possono attraversare al massimo 2 ripetitori;
- il ripetitore in fibra ottica conta come mezzo ripetitore;
- la lunghezza massima di un link in fibra ottica è di 1000 m;
- qualora in una LAN ci siano più link in fibra ottica, la lunghezza aggregata di due qualunque di essi non deve superare i 1000 m.

Per facilitare il compito di chi progetta, si consiglia di considerare un segmento coax come dorsale, a cui si collegano sia dei segmenti locali tramite ripetitori locali sia dei segmenti remoti tramite delle coppie di half-repeater.

La violazione delle regole sopra esposte può comportare dei malfunzionamenti della rete e la presenza di pacchetti corrotti (ad esempio, *misaligned packet* o *giant packet*).

Le figure 6.9 e 6.10 mostrano degli esempi di configurazione.

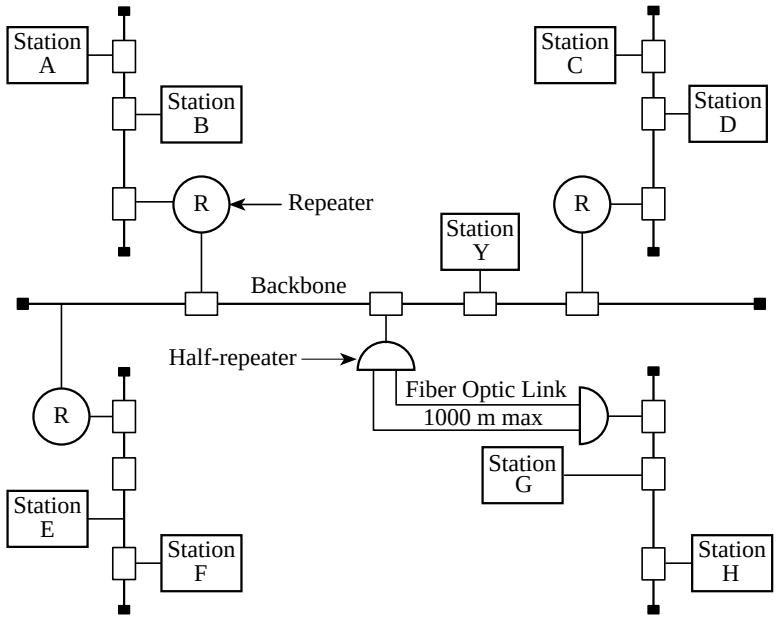


Fig. 6.9 - Esempio di configurazione massima con Ethernet.

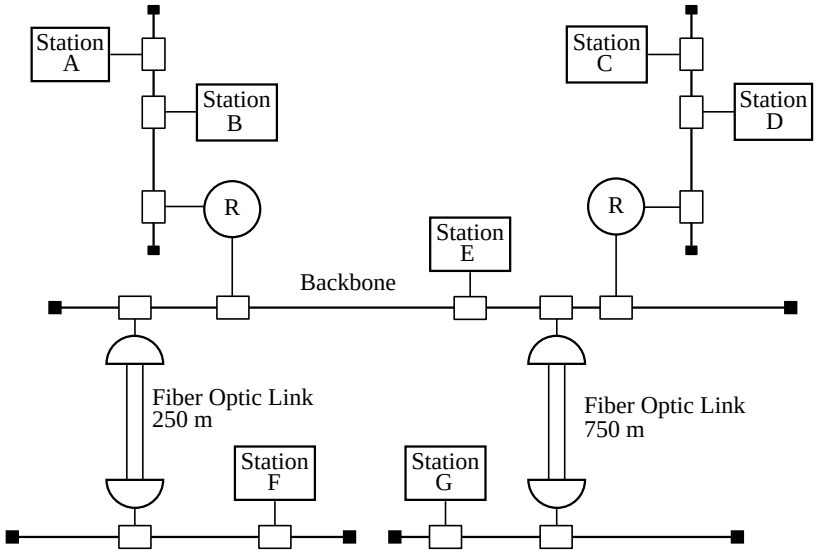


Fig. 6.10 - Esempio di configurazione con due coppie di half-repeater.

6.4 LO STANDARD IEEE 802.3/ISO 8802.3

Lo standard 8802.3 si colloca al livello 1 della pila OSI e al sottolivello MAC del livello 2, mentre il Logical Link Control è demandato allo standard 8802.2. Le figure 6.1 e 6.11 mostrano le relazioni tra i livelli di riferimento OSI.

IEEE 802.3 nasce come architettura a bus su cavo coassiale ed evolve successivamente verso topologie a stella basate sull'utilizzo di cavi UTP e fibre ottiche. Le velocità trasmissive sono 1 Mb/s (versione 1Base5) e 10 Mb/s (versioni 10Base5, 10Base2, 10BaseT, 10BaseF, 10Broad36), e il metodo di accesso è il CSMA/CD.

In questo paragrafo tratteremo soltanto la trasmissione a 10 Mb/s che è quella più usata e conosciuta. Non tratteremo la versione 10Broad36, che utilizza tecniche in radio frequenza su cavo CATV (CAble TV), in quanto è una tecnica molto costosa ed attualmente in disuso.

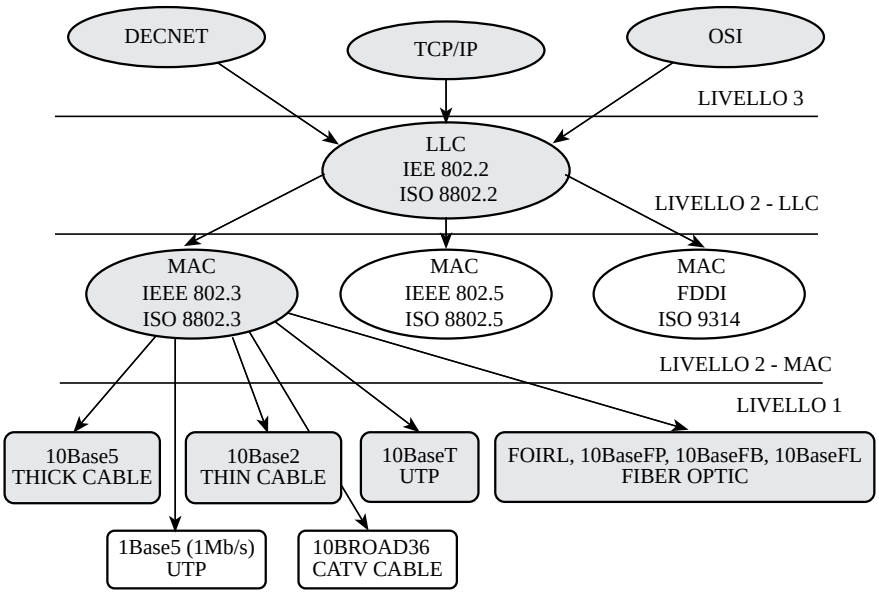


Fig. 6.11 - Relazioni tra 802.3 e i livelli OSI.

6.4.1 Livello Fisico

Il livello Fisico si occupa principalmente di codificare i pacchetti in stringhe seriali di bit e decodificare stringhe seriali di bit in pacchetti secondo la codifica Manchester (si veda il paragrafo 3.1.2). Nel livello Fisico sono contenute le caratteristiche dei segnali e degli elementi che vi operano quali transceiver, ripetitori, cavi e connettori.

Le principali caratteristiche relative al livello Fisico sono:

- velocità trasmissiva 10 Mb/s;
- 4 km di distanza massima ammessa tra le due stazioni più distanti (caso di 2 link in fibra ottica 10BaseFL da 2 km ciascuno, con due stazioni connesse agli estremi ed un ripetitore interposto tra i link in fibra ottica);
- un massimo di 1024 stazioni collegabili;
- mezzi trasmissivi ammessi: cavo coassiale di tipo thick, cavo coassiale di tipo thin, doppini, fibre ottiche multimodali, cavo CATV;
- topologie ammesse: bus, punto-punto, stella.

6.4.2 Sottolivello MAC

Le principali funzioni dello standard 802.3 relative al sottolivello MAC sono quelle già descritte nel paragrafo 6.2.

I parametri principali del sottolivello MAC sono i riportati in tabella 6.2.

Slot time	512 bit time (51.2 μs)	tempo base di attesa prima di una ritrasmissione
Inter Packet Gap	9.6 μs	distanza minima tra due pacchetti
Attempt limit	16	massimo numero di tentativi di ritrasmissione
Backoff limit	10	numero di tentativi oltre il quale non aumenta più la casualità del back-off
Jam size	32 bit	lunghezza della sequenza di jam
Max frame size	1518 ottetti	lunghezza massima del pacchetto
Min frame size	64 ottetti (512 bit)	lunghezza minima del pacchetto
Address size	48 bit	lunghezza indirizzi MAC

Tab. 6.2 - IEEE 802.3: principali parametri.

Il pacchetto 802.3 (figura 6.12) ha una lunghezza variabile compresa tra 64 e 1518 ottetti, in testa al pacchetto c'è un preambolo di 7 ottetti che serve alla stazione ricevente per sincronizzarsi sul clock di quella trasmittente, immediatamente dopo c'è un ottetto di SFD (*Start Frame Delimiter* codificato con la sequenza di bit 11010101) che indica l'inizio del pacchetto.

Nel campo di *destination address* è contenuto l'indirizzo della stazione a cui è destinato il pacchetto, nel campo di *source address* è contenuto l'indirizzo della stazione che ha originato il pacchetto.

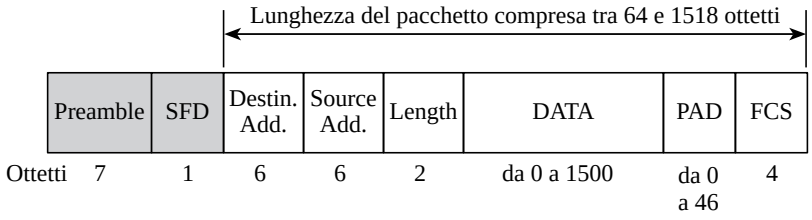


Fig. 6.12 - Formato del pacchetto 802.3.

Il campo di *length* indica il numero di ottetti contenuti nel campo *data*, il *PAD* viene appeso in coda al precedente campo solo se quest'ultimo è più corto di 46 ottetti e contiene un numero di ottetti calcolato in modo da garantire che venga rispettata la lunghezza minima del pacchetto (64 ottetti).

Il campo *data* contiene le LLC-PDU, il campo FCS (*Frame Check Sequence*) contiene il valore di CRC calcolato sulla base dei campi descritti precedentemente.

Come in Ethernet 2.0 non esiste un segnalatore di fine pacchetto: tale ruolo è assunto dall'Inter Packet Gap, la cui durata non può quindi scendere sotto il valore minimo fissato in 9.6 μs.

6.4.3 Mezzi trasmissivi

I diversi mezzi trasmissivi ammessi verranno trattati nei relativi paragrafi dedicati alle varie versioni dello standard, e cioè 10Base5 e 10Base2 per i cavi coassiali, 10BaseT per i doppini e 10BaseF per le fibre ottiche.

6.4.4 Transceiver

I transceiver variano a seconda del mezzo trasmissivo che interfacciano ed a seconda delle specifiche relative ai supplementi di 802.3. Le funzioni principali sono le stesse già spiegate nel paragrafo 6.3.4, ad eccezione della differenza di tempistica del segnale di heartbeat che ora assume anche un altro nome - SQE test (*Signal Quality Error test*) - e della possibilità di abilitare o disabilitare questo segnale. I transceiver sono anche detti MAU (*Medium Attachment Unit*) e sono composti da due parti: la PMA (*Physical Medium Attachment*) e la MDI (*Medium Dependent Interface*).

6.4.5 Interfaccia 802.3

Il controller 802.3 ha le stesse funzioni del controller Ethernet, ma a differenza di questo può avere il transceiver integrato al suo interno.

Il segnale di SQE test è incompatibile tra un transceiver Ethernet v.2.0 e un controller 802.3 e viceversa; nel caso di connessione tra due elementi incompatibili si possono verificare delle false collisioni ed è quindi preferibile disabilitare l'heartbeat sul transceiver, pur perdendo così la verifica del test di collisione.

La figura 6.13 mostra le differenze di tempistica dell'Heartbeat tra Ethernet e 802.3.

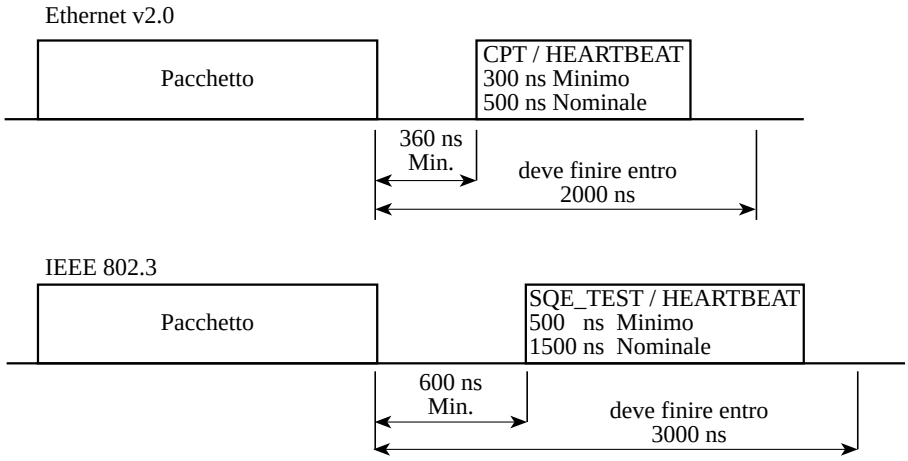


Fig. 6.13 - Tempistiche dell'heartbeat.

6.4.6 Cavo AUI

Il cavo AUI (*Attachment Unit Interface*) ha le stesse funzioni del cavo transceiver per Ethernet, ma a differenza di questo ha un più appropriato collegamento degli schermi (calza e foglio di alluminio) per cui è più immune ai disturbi.

6.4.7 Repeater 802.3

Il ripetitore lavora a livello Fisico e ripete i segnali, ricevuti su un segmento, a tutti gli altri segmenti; la figura 6.14 mostra il ruolo di un ripetitore per l'interconnessione di due segmenti all'interno del modello di riferimento OSI.

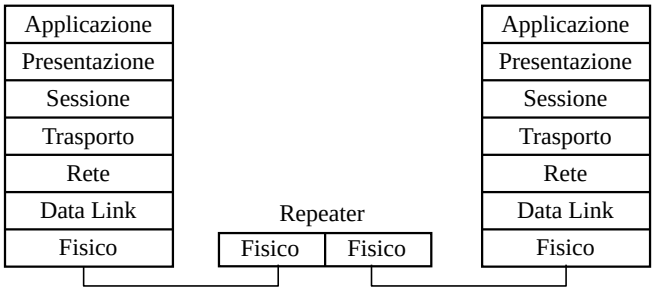


Fig. 6.14 - Relazione tra un ripetitore ed i livelli OSI.

Il ripetitore 802.3 è diverso da quello Ethernet in quanto rigenera il preambolo e richiede che il SQE test venga disabilitato sui transceiver ad esso connessi.

Le funzioni principali di un ripetitore 802.3 sono le seguenti:

- ripete le stringhe di bit ricevuti su un segmento e le trasmette sugli altri segmenti con un'ampiezza di segnale appropriata;
- assicura che la simmetria dei segnali sia entro la tolleranza richiesta dalle specifiche del MAU (transceiver);
- decodifica, secondo il metodo Manchester, le stringhe seriali di bit ricevute su una porta e le ricodifica prima di ritrasmetterle sulle altre porte, ritemporizzando quindi tutti i bit da trasmettere;
- si occupa della gestione della collisione: se viene rilevata su una qualunque porta, il ripetitore trasmette la sequenza di jam di 96 bit su tutte le porte; tale sequenza serve a garantire la propagazione della collisione su tutti i segmenti;
- rigenera il preambolo: il ripetitore deve trasmettere un minimo di 56 bit di preambolo seguiti dallo SFD;
- quando riceve un frammento di collisione inferiore a 96 bit incluso il preambolo, estende questo frammento con una sequenza di jam in modo che il numero di bit ritrasmessi sia uguale a 96;
- protegge i segmenti connessi ad esso da errori di *jabber* (pacchetti troppo lunghi); quando si accorge che sta trasmettendo una stringa di bit per un periodo continuativo superiore a 5 ms interrompe la trasmissione e la riabilita dopo un tempo che va da 9.6 a 11.6 ms;
- può opzionalmente isolare una porta (e quindi partizionare la rete), per un determinato periodo di tempo, quando su questa si verificano più di 30 collisioni consecutive;
- il ripetitore può ospitare al suo interno i transceiver integrati.

Le figure 6.15 e 6.16 mostrano esempi di circuiti logici di un ripetitore multiporta.

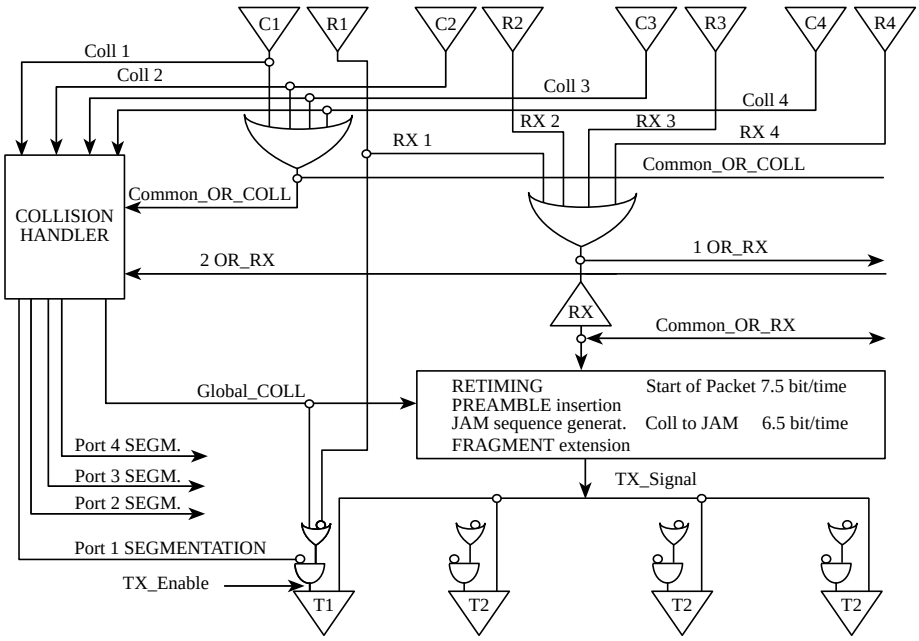


Fig. 6.15 - Esempio di ripetitore multiporta.

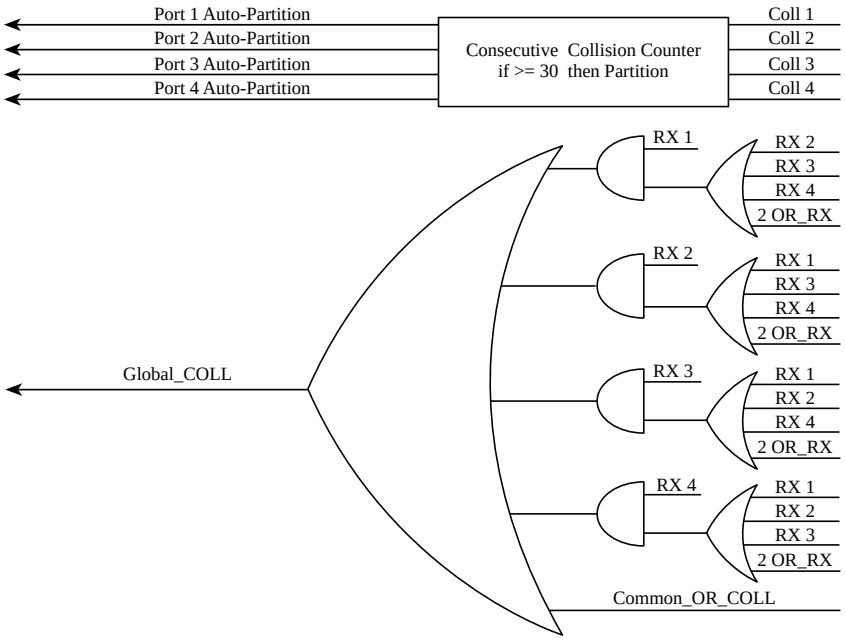


Fig. 6.16 - Circuito di un ripetitore per la gestione della collisione.

6.4.8 10Base5 - Coax

Le specifiche di questo standard riguardano le caratteristiche dei MAU e dei mezzi trasmissivi che sono relative alla velocità trasmissiva di 10 Mb/s (numero indicato nel primo campo del nome dello standard) e sono basate su un segmento di 500 m (5 unità da 100 m, numero indicato nel secondo campo del nome dello standard) dove si connettono le stazioni.

Il MAU 10Base5 è in grado di trasmettere e ricevere dei segnali elettrici lungo un segmento coassiale thick di 500 m. Le caratteristiche principali sono quelle riportate nel paragrafo 6.3.4. L'elemento MDI (Medium Dependent Interface) è costituito dai circuiti driver e receiver per il cavo coassiale (figura 6.6) e da un sistema di accoppiamento meccanico chiamato tap (figura 6.7).

Il segmento 10Base5 è costituito da un cavo coassiale da 50 Ω di tipo RG213 (chiamato anche "cavo thick" o "cavo giallo" o "cavo Ethernet"), le cui specifiche sono le stesse richieste dall'Ethernet v. 2.0, riportate nel paragrafo 6.3.3.

Le regole di configurazione riguardanti il singolo segmento da 500 m sono le stesse di Ethernet v. 2.0 e sono riassunte nella figura 6.17.

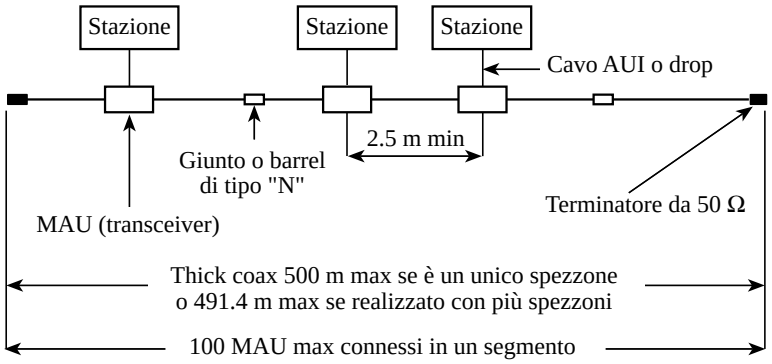

Stazione
Stazione
Stazione
Cavo AUI o drop
2.5 m min
Giunto o barrel
di tipo "N"
Terminatore da 50 Ω
MAU (transceiver)
Thick coax 500 m max se è un unico spezzone
o 491.4 m max se realizzato con più spezzoni
100 MAU max connessi in un segmento

Fig. 6.17 - Regole di configurazione del segmento 10Base5.

6.4.9 10Base5 - FOIRL

Alternativamente al cavo coassiale e al relativo MAU è possibile utilizzare fibra ottica e un FOMAU (Fiber Optic MAU). Il FOMAU (chiamato normalmente MAU o transceiver FOIRL) è in grado di trasmettere e ricevere segnali ottici lungo un segmento in fibra ottica di lunghezza massima pari a 1000 m; questo segmento è di tipo link e viene chiamato con il nome di FOIRL (Fiber Optic Inter Repeater Link). Il FOMAU è composto da un FOPMA (Fiber Optic Physical Medium

Attachment) e da un FOMDI (Fiber Optic Medium Dependent Interface) che è costituito dagli emettitori basati su LED, dai ricevitori e dai connettori che sono utilizzati per connettere fisicamente la fibra ottica (figura 6.18).

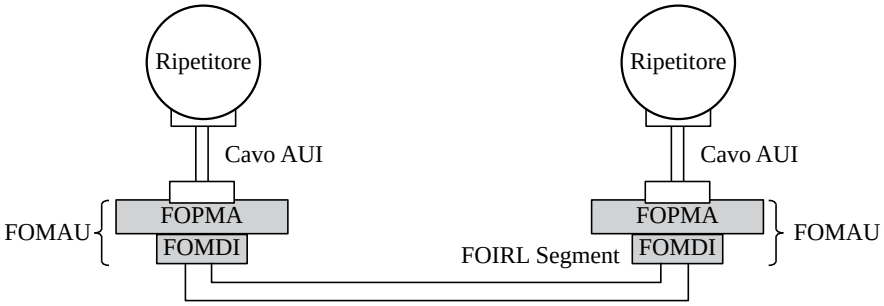


Fig. 6.18 - Interconnessione FOIRL.

Le fibre ottiche ammesse sono le seguenti: 50/125, 62.5/125, 85/125 e 100/140; quella preferita è 62.5/125. Le caratteristiche richieste sono quelle specificate dallo standard EIA/TIA 568.

Le funzioni principali del FOMAU sono le seguenti:

- funzione di trasmissione: la stringa di bit ricevuta dal ripetitore viene trasmessa sulla fibra ottica;
- funzione di ricezione: la stringa di bit ricevuta dalla fibra ottica viene trasmessa al ripetitore;
- funzione di rilevamento della collisione;
- funzione di *optical-idle*: in assenza di dati trasmette un segnale di idle che consiste in una sequenza periodica di impulsi ottici aventi una frequenza di 1 MHz con tolleranza +25% -15%;
- funzione di *jabber*: quando il FOMAU riceve dall'interfaccia una stringa di bit di lunghezza superiore alla massima interrompe la funzione di trasmissione;
- funzione di *low light level detection*: quando riceve dei segnali ottici di intensità inferiore ad una certa soglia di sicurezza interrompe la funzione di ricezione.

Le caratteristiche ottiche del FOMAU sono le seguenti:

- trasmissione sulla fibra ottica tramite l'impiego di LED che lavorano alla lunghezza d'onda di 850 nm;
- valore di picco del segnale ottico trasmesso: -12 dBm ± 2 dB misurato con un accoppiamento tramite fibra ottica 62.5/125 μm;
- sensibilità del ricevitore: da -27 a -9 dBm;

Il *power budget* che si ha a disposizione sul link è di 13 dB; questo è il risultato della differenza tra il segnale di picco trasmesso con il limite di tolleranza peggiore, e la sensibilità massima del ricevitore: 27 - 14 = 13 dB. A questo valore bisogna sottrarre 1 dB di tolleranza sull'accoppiamento della fibra ottica, più 3 dB di margine per il degrado della sorgente ottica dovuto al tempo di vita del LED, per cui si ottiene un budget reale di 9 dB.

I connettori utilizzati sono il tipo "ST" per le fibre ottiche con il cladding da 125µm (50/125, 62.5/125) e il tipo "F-SMA" per la fibra 100/140.

6.4.10 10Base2

Le specifiche di questo standard riguardano le caratteristiche dei MAU e dei mezzi trasmissivi per la velocità di 10 Mb/s (numero indicato nel primo campo del nome dello standard) e sono basate su un segmento di 185 m (circa 2 unità da 100 m, numero indicato nel secondo campo del nome dello standard) dove si connettono le stazioni.

Il MAU (transceiver) 10Base2 è in grado di trasmettere e ricevere dei segnali elettrici lungo un segmento coassiale thin di 185 m. Le caratteristiche principali sono quelle riportate nel paragrafo 6.3.4. L'elemento MDI (Medium Dependent Interface) è costituito dai circuiti driver e receiver per il cavo coassiale (figura 6.19) e da un sistema di accoppiamento meccanico basato sul connettore a "T" di tipo BNC

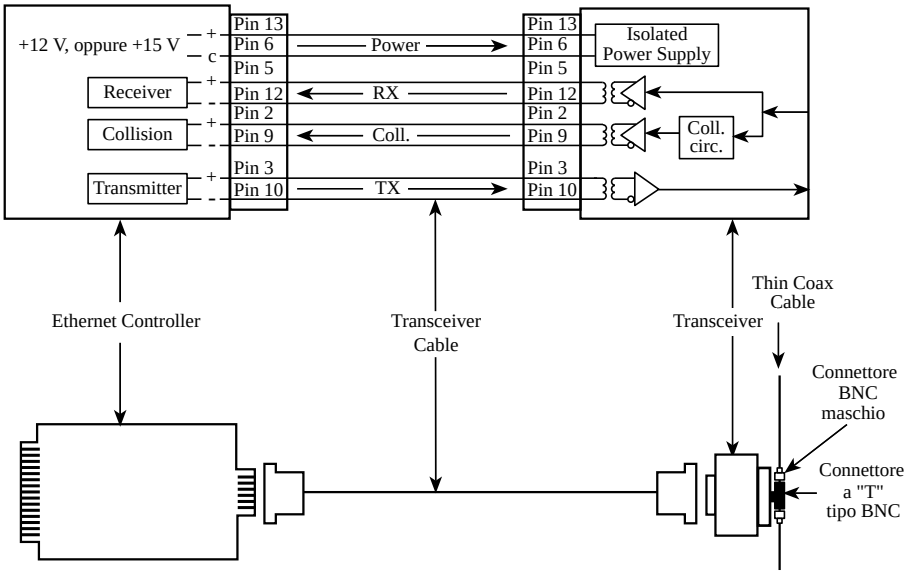


Fig. 6.19 - Connessioni del transceiver 10Base2.

Il segmento 10Base2 è costituito da un cavo coassiale da 50 Ω di tipo RG58 A/U o C/U (chiamato anche cavo "thin" o "Ethernet sottile"), le cui specifiche minime richieste sono le seguenti:

- impedenza 50 ± 2 Ω;
- velocità di propagazione minima 0.65 c, dove c è la velocità della luce;
- attenuazione massima del segmento (185 m) 8.5 dB a 10 MHz e 6 dB a 5 MHz.

Le regole di configurazione riguardanti il segmento coassiale sono:

- la lunghezza massima del segmento coassiale è di 185 m;
- la lunghezza massima di un cavo transceiver è di 50 m;
- la distanza minima tra due transceiver è di 0.5 m;
- il numero massimo di transceiver collegabili in un segmento è 30.

La figura 6.20 mostra le regole di configurazione del segmento 10Base2.

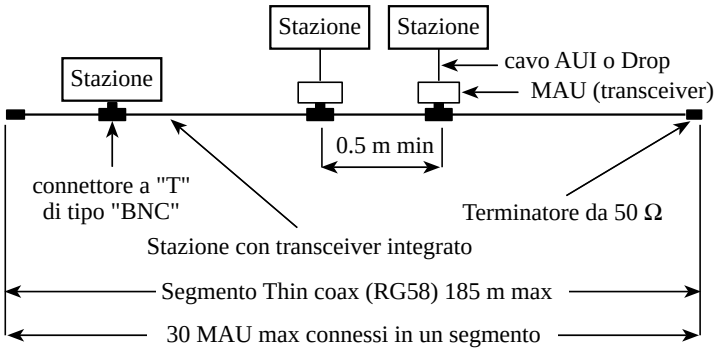


Fig. 6.20 - Regole di configurazione del segmento 10Base2.

6.4.11 10BaseT

Le specifiche di questo standard riguardano le caratteristiche dei MAU e dei mezzi trasmissivi alla velocità di 10 Mb/s (numero indicato nel primo campo del nome dello standard) su un segmento di Twisted Pair (doppino) come indicato dalla "T" presente nel secondo campo del nome dello standard. 10BaseT ammette la connessione di due sole stazioni in modalità punto-punto. La particolarità di questo standard implica l'utilizzo di ripetitori multiporta per poter connettere più di due stazioni in rete e la topologia è quindi di tipo stellare. Pertanto, data l'esatta corrispondenza di specifiche con gli standard per i cablaggi strutturati sia in termini

di topologia che in termini di caratteristiche elettriche dei mezzi trasmissivi, lo standard 10BaseT è particolarmente adatto per essere utilizzato in tali installazioni.

Il MAU (transceiver) 10BaseT è in grado di trasmettere e ricevere dei segnali elettrici lungo un segmento di doppino (normalmente UTP di categoria 3 o superiore) di circa 100 m. L'elemento MDI (Medium Dependent Interface) è costituito dai circuiti driver e receiver per il doppino e da una presa RJ45 (jack a 8 contatti con chiave centrale). La figura 6.21 mostra l'assegnazione dei contatti (assegnazione che corrisponde alle coppie 2 e 3 degli standard per i cablaggi strutturati).

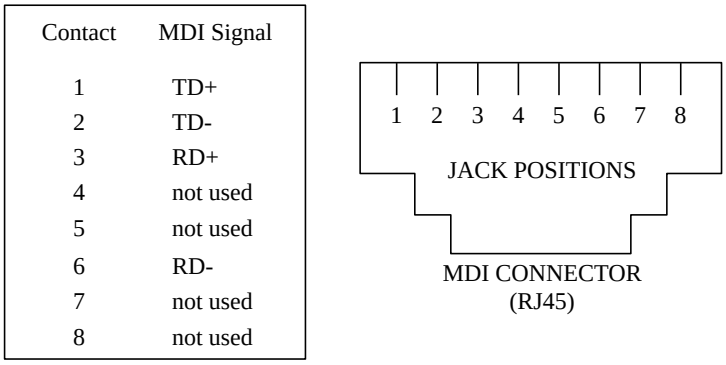


Fig. 6.21 - Assegnazione dei contatti su RJ45.

Le funzioni principali del MAU 10BaseT sono:

- funzione di trasmissione: trasferisce i dati codificati secondo la codifica Manchester dal circuito DO (*Data Output*) alla coppia di trasmissione TD (*Transmit Data*); se sul circuito DO non c'è alcuna trasmissione in corso trasmette sulla coppia TD un segnale di idle detto TP_IDL;
- funzione di ricezione: trasferisce i dati codificati ricevuti sulla coppia RD (*Receive Data*) al circuito DI (*Data In*);
- funzione di rilevamento della collisione: quando rileva simultaneamente la presenza di dati sia sulla coppia RD che sul circuito DO, riporta un segnale di collisione sul circuito CI (*Collision In*);
- *SQE test*: invia un segnale di test del circuito di rilevazione delle collisioni sul circuito CI alla fine della trasmissione del pacchetto;
- funzione di *jabber*: quando riceve una stringa di dati da DO superiore alla lunghezza massima ammessa del pacchetto 802.3 interrompe la funzione di trasmissione;

- funzione di *loopback*: durante il trasferimento dei dati dal circuito DO alla coppia TD esegue anche lo stesso trasferimento dei dati verso il circuito DI;
- funzione di *link integrity test*: protegge la rete dalle conseguenze di un'eventuale rottura del link RD; se in un intervallo di tempo compreso tra 50 e 150 ms il MAU non riceve dei dati oppure il segnale TP_IDL, entra in uno stato di *link test fail*.

Il segnale di TP_IDL è composto da uno *start of TP_IDL* seguito da un'alternanza di silenzi aventi un periodo compreso tra 8 e 24 ms e di impulsi di *link test*. La figura 6.22 mostra il segnale TP_IDL.

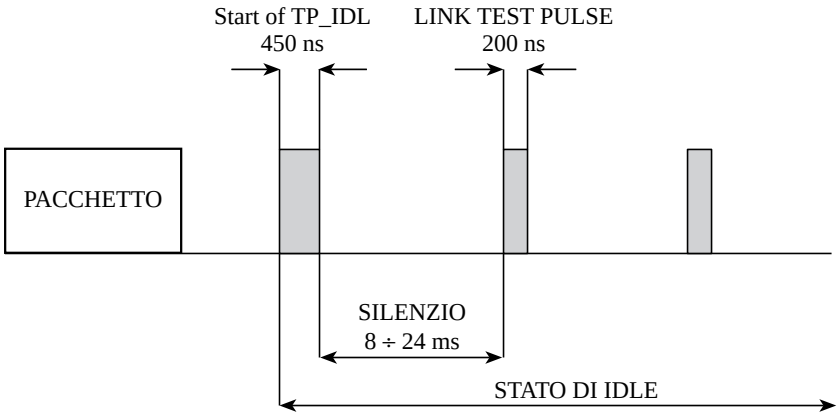


Fig. 6.22 - Segnale di idle.

Quando il MAU è integrato dentro un ripetitore multiporta è consigliabile che adotti l'incrocio delle coppie (crossover) così si può eseguire un cablaggio senza inversioni tra il ripetitore ed il MAU della stazione (figura 6.23).

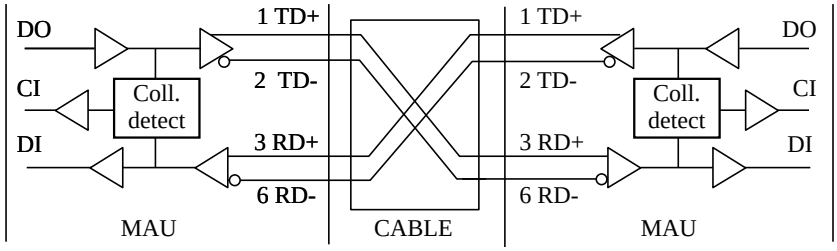


Fig. 6.23 - Connessioni tra due MAU 10BaseT.

Il segmento 10BaseT è costituito da un cavo avente come minimo due coppie ritorte da 100 Ω con le seguenti caratteristiche minime:

- impedenza 100 ± 15 Ω misurata alle frequenze comprese tra 1 e 16 MHz;
- velocità di propagazione minima 0.585 c, dove c è la velocità della luce;
- attenuazione massima del segmento, includendo cavi e connettori, 11.5 dB nelle frequenze comprese tra 5 e 10 MHz;
- valore minimo richiesto di attenuazione di diafonia tra le coppie (NEXT) per un cavo UTP a 4 coppie: 26 - 15 $\log_{10}(f/10)$ dB nell'intervallo di frequenza compreso tra 5 e 10 MHz, dove "*f*" è la frequenza espressa in MHz;
- valore minimo richiesto di attenuazione di diafonia tra le coppie (NEXT) per un cavo UTP a 25 coppie: 30 - 15 $\log_{10}(f/10)$ dB nell'intervallo di frequenza compreso tra 5 e 10 MHz, dove "*f*" è la frequenza espressa in MHz.

Normalmente la lunghezza del segmento da considerare è di 100 m, ma potrebbe anche aumentare qualora i valori relativi alla somma di tutte le attenuazioni dei singoli componenti e le considerazioni sulla diafonia combinata di tutti i componenti rientrino nei limiti sopra descritti. Ad esempio, utilizzando dei cavi di categoria 5 e dei connettori di cat. 4 o 5 il segmento 10BaseT può raggiungere una lunghezza di 160 m.

Il modello di riferimento di una connessione 10BaseT è mostrato in figura 6.24.

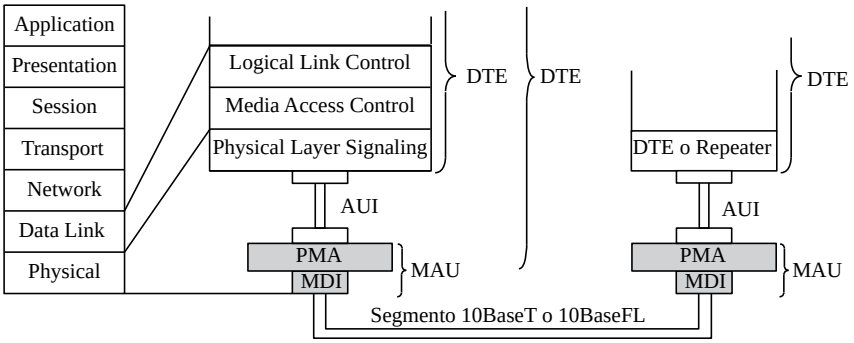


Fig. 6.24 - Interconnessione 10BaseT o 10BaseFL.

6.4.12 10BaseF

Lo standard 10BaseF si occupa di regolamentare l'utilizzo della fibra ottica come mezzo trasmissivo per LAN 802.3. Esso si suddivide in tre sotto-standard che sono:

- 10BaseFP basato sull'utilizzo di stelle ottiche passive;

- 10BaseFB basato su una trasmissione sincrona sulla fibra ottica;
- 10BaseFL compatibile con il precedente standard FOIRL, ma notevolmente migliorato.

A ciascuno di questi verrà dedicato un apposito paragrafo.

Tutti i tre sotto-standard si uniformano alle specifiche EIA/TIA 568 per ciò che riguarda la fibra ottica ed i componenti passivi; i LED utilizzati lavorano sulla lunghezza d'onda di 850 nm.

6.4.13 10BaseFP

Le specifiche di questo standard riguardano le caratteristiche dei MAU e dei mezzi trasmissivi per la velocità di 10 Mb/s (numero indicato nel primo campo del nome dello standard) su segmenti in fibra ottica connessi tramite una stella passiva (FP: *Fiber Passive*).

I promotori di questo standard, tra cui ricordiamo la Codenoll, hanno pensato di adottare una soluzione che fosse un'alternativa al cavo coassiale in cui però gli unici elementi attivi del segmento fossero i transceiver ottici. Con la fibra ottica si possono realizzare solo collegamenti punto-punto: quindi per poter connettere più di due stazioni si è fatto uso di stelle passive. Una stella passiva è basata sul concetto dello splitter ottico, ovvero un ripartitore di segnale luminoso; questa tecnica implica che gran parte del segnale luminoso vada perso nella stella e per questo motivo è necessario che i transceiver abbiano un'elevata dinamica. La lunghezza massima di fibra ottica che si può avere tra la stella ottica passiva ed il MAU è di 500 m, la distanza massima tra due MAU che sono interconnessi tramite una stella è di 1000 m.

La figura 6.25 mostra il modello di riferimento dello standard 10BaseFP.

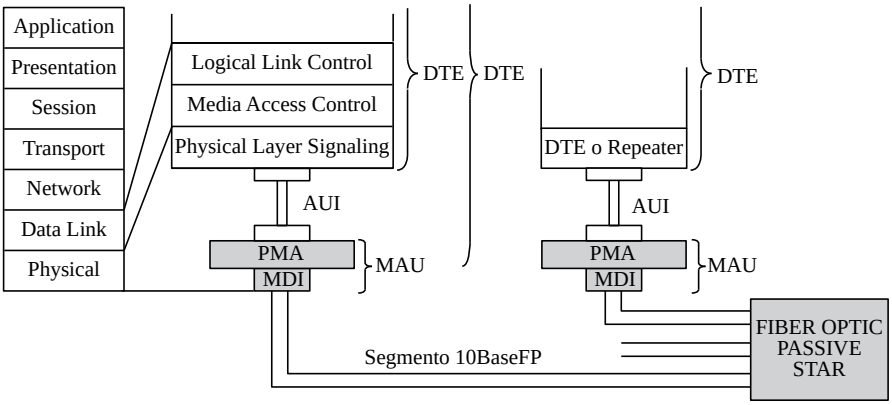


Fig. 6.25 - Interconnessione 10BaseFP.

6.4.14 10BaseFB

Le specifiche di questo standard riguardano le caratteristiche dei MAU e dei mezzi trasmissivi per la velocità di 10 Mb/s (numero indicato nel primo campo del nome dello standard) su segmenti in fibra ottica con funzione di dorsale tra due ripetitori (FB: *Fiber Backbone*).

I promotori di questo standard, tra cui ricordiamo la Chipcom e la Lannet, hanno pensato di adottare una soluzione che fosse un'alternativa al cavo coassiale in cui però gli elementi attivi del segmento fossero sia i transceiver ottici, sia le stelle attive.

Una delle prime bozze identificava questo standard con il nome 10BaseFA (*Fiber Active*) in quanto permetteva sia la connessione di ripetitori, sia di stazioni. Il comitato IEEE ha poi limitato lo standard definitivo a semplici funzioni di dorsale: è quindi possibile utilizzare dei segmenti 10BaseFB soltanto per interconnettere due ripetitori. Questa limitazione non ha ragioni di tipo funzionale e aziende come la Chipcom e la Lannet producono ancora oggi transceiver compatibili alle specifiche 10BaseFB che servono per interconnettere le stazioni alle stelle attive.

Lo standard 10BaseFB, essendo di tipo sincrono, si presta meglio di altri alla costruzione di transceiver fault-tolerant; questi transceiver sono dotati di 2 porte in fibra ottica, di cui una *main* ed una *backup*. Nel caso di un guasto sul main link il transceiver commuta in breve tempo (circa 20 ms) sulla porta di backup.

Non è possibile scindere fisicamente il MAU dal ripetitore in quanto formano un unico insieme, come mostrato in figura 6.26.

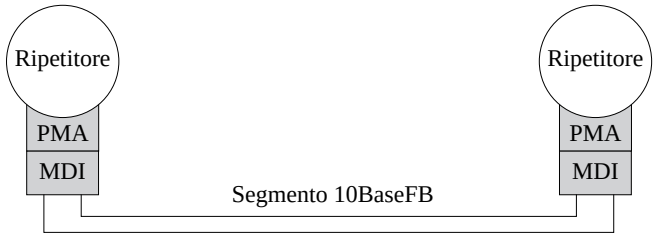


Fig. 6.26 - Modello di riferimento 10BaseFB.

Le caratteristiche principali del MAU 10BaseFB sono le seguenti:

- la velocità trasmissiva è di 10 Mb/s;
- opera su un segmento in fibra ottica che può avere una lunghezza massima di 2000 m;

- trasmette i dati ed il segnale di idle in modo sincrono con i bit di clock e quindi riceve i dati senza aver bisogno di risincronizzarsi su ogni pacchetto;
- prevede una connessione point-to-point tra due ripetitori, e permette dei cablaggi a topologia stellare quando è utilizzato con ripetitori multiporta.

Le funzioni principali del MAU sono le seguenti:

- trasmette i messaggi ricevuti dal ripetitore sulla fibra ottica; questa funzione si suddivide in tre sottofunzioni: conversione dei segnali elettrici in ottici, generazione del segnale SIDL (*Synchronous IDLe*) quando riceve il messaggio di output idle dal ripetitore, generazione del segnale RF (*Remote Fault*) in caso di guasto del link;
- in assenza di dati trasmette il segnale di synchronous idle che serve per mantenere sempre agganciati in frequenza i transceiver posti ai due estremi di un segmento in fibra ottica; esso ha una frequenza costante di 2.5 MHz (figura 6.27);
- in caso di ricezione con presenza di anomalie quali: *jabber* (pacchetto di lunghezza superiore al massimo consentito), *low-light* (segnale ottico insufficiente), *invalid data* (dati non validi), *lock-lost* (perdita della sincronizzazione), trasmette il segnale di *remote-fault* che ha una frequenza di 1.667 MHz (figura 6.27);
- riceve i segnali ottici dalla fibra ottica e trasmette i messaggi al ripetitore; questa funzione si suddivide in due sottofunzioni: conversione dei segnali ottici in elettrici, rilevazione dei segnali di SIDL e RF e interpretazione di quelli RF;
- rileva la collisione nel caso in cui ci sia simultaneità di ricezione del segnale d'ingresso del ripetitore e di quello di uscita verso il MAU;
- le funzioni di *jabber* e di *loopback* sono simili a quelle degli altri tipi di MAU;
- la funzione di gestione delle condizioni di guasti (*fault condition*) che possono essere: *low light, receive jabber, invalid data* e *remote fault*.

Caratteristiche ottiche del MAU 10BaseFB sono:

- trasmissione sulla fibra ottica tramite l'impiego di LED che lavorano alla lunghezza d'onda di 850 nm;
- valore del segnale ottico trasmesso: da -20 a -12 dBm misurato con un accoppiamento tramite fibra ottica 62.5/125;
- sensibilità del ricevitore: da -32.5 a -12 dBm.

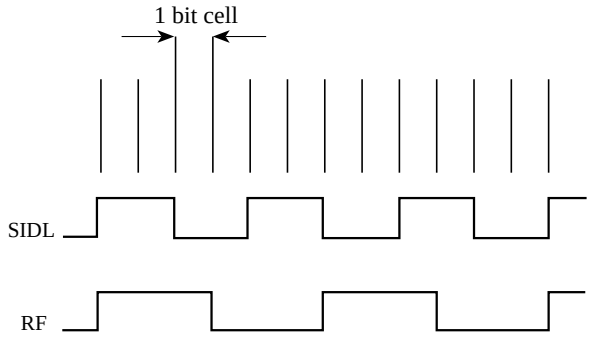


Fig. 6.27 - Codifica dei segnali SIDL e RF.

Il power budget che si ha a disposizione sul link è di 12.5 dB; questo è il risultato della differenza tra il segnale di picco trasmesso con il limite di tolleranza peggiore, e la sensibilità massima del ricevitore: 32.5 - 20 = 12.5 dB.

Le regole di configurazione riguardanti il segmento 10BaseFB sono:

- può solo interconnettere due ripetitori e quindi le connessioni alle stazioni non sono ammesse;
- la lunghezza massima del segmento è di 2000 m.

Dal momento che non è necessario risincronizzarsi su ogni pacchetto ricevuto, il ripetitore non necessita di rigenerare i bit persi del preambolo poiché, essendo il MAU ricevente agganciato perfettamente in frequenza con quello trasmittente, non si ha perdita di bit. Non c'è il rischio di riduzione dell'Inter Packet Gap dovuta alla perdita di alcuni bit del preambolo, e questo permette di poter avere parecchi segmenti 10BaseFB in cascata.

6.4.15 10BaseFL

Le specifiche di questo standard riguardano le caratteristiche dei MAU e dei mezzi trasmissivi per la velocità di 10 Mb/s (numero indicato nel primo campo del nome dello standard) su segmenti in fibra ottica di tipo link (FL: *Fiber Link*) cioè per interconnettere ripetitori e stazioni in modalità punto-punto e stellare.

Il modello di riferimento di una connessione 10BaseFL è mostrato in figura 6.24.

Le caratteristiche principali del MAU 10BaseFL sono le seguenti:

- la velocità trasmissiva è di 10 Mb/s;
- opera su un segmento in fibra ottica che può avere una lunghezza massima di 2000 m;
- permette al DTE o al ripetitore di verificare la connessione al MAU e di questo al mezzo trasmissivo tramite un segnale OPT_IDL;
- prevede una connessione punto-punto tra due MAU, e permette dei cablaggi a topologia stellare quando è utilizzato con dei ripetitori multiporta.

Funzioni principali del MAU 10BaseFL:

- funzione di trasmissione: trasferisce i dati codificati secondo la codifica Manchester dal circuito DO (*Data Output*) alla fibra ottica trasmittente (OTD, figura 6.28); se sul circuito DO non c'è alcuna trasmissione in corso trasmette sulla fibra ottica un segnale di idle detto OPT_IDL;
- funzione di ricezione: trasferisce i dati codificati ricevuti sulla fibra ottica (ORD) al circuito DI (*Data Input*);
- funzione di rilevamento della collisione: quando rileva simultaneamente la presenza di dati sia sulla fibra ottica ricevente (ORD) che sul circuito DO, riporta un segnale di collisione sul circuito CI (*Collision Input*);
- *Signal Quality Error (SQE) test*: invia un segnale di test del circuito di rilevazione delle collisioni sul circuito CI alla fine della trasmissione del pacchetto;
- funzione di *jabber*: quando riceve una stringa di dati da DO superiore alla lunghezza massima ammessa del pacchetto 802.3 interrompe la funzione di trasmissione;
- funzione di *loopback*: durante il trasferimento dei dati dal circuito DO alla fibra ottica trasmittente OTD esegue anche lo stesso trasferimento dei dati verso il circuito DI;
- funzione di *link integrity test*: protegge la rete dalle conseguenze di un'eventuale rottura del link ORD; se si verifica una condizione di *low-light level*, entra in uno stato di *link test fail*;
- segnalazione di *low-light level*: diventa attiva quando il segnale ottico in ricezione (ORD) scende sotto la soglia di -32.5 dBm.

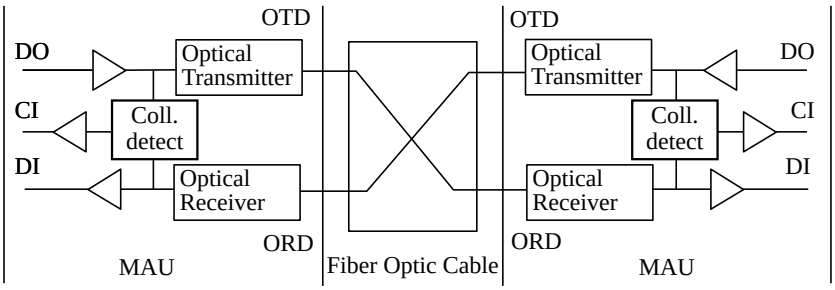


Fig. 6.28 - Connessioni tra due MAU 10BaseFL.

Il segnale di OPT_IDL è composto da uno *start of OPT_IDL* seguito da una sequenza di impulsi ottici periodici aventi una frequenza di 1 MHz con tolleranza +25% -15%.

Il segmento 10BaseFL consiste in una connessione punto-punto in fibra ottica tra due MAU, le cui regole di configurazione sono:

- può interconnettere sia ripetitori, sia stazioni;
- la lunghezza massima del segmento è di 2000 m.

Il MAU 10BaseFL è compatibile con il MAU FOIRL, ma quando è connesso ad esso la lunghezza del segmento si riduce a 1000 m. Le caratteristiche ottiche sono uguali a quelle dei MAU 10BaseFB.

6.5 PARAMETRI DI CONFIGURAZIONE PER LE RETI IEEE 802.3

Per configurare correttamente una LAN 802.3, oltre a rispettare la lunghezza massima di ogni tipo di segmento, occorre porre dei limiti sul numero e sulla tipologia dei segmenti e sul numero dei ripetitori.

Tali limiti sono dettati da alcune considerazioni sui due parametri principali su cui si basa il protocollo, e cioè l'*Inter Packet Gap* e il *Round Trip Delay*.

6.5.1 Inter Packet Gap

Come già visto, nelle reti locali Ethernet/IEEE 802.3 i pacchetti MAC non hanno un delimitatore di fine trama, ma è l'*Inter Packet Gap* (IPG) che li delimita. Se l'IPG subisce una forte riduzione questo può portare due pacchetti

ad incollarsi e a diventare indistinguibili. La riduzione dell'IPG può avvenire perché i pacchetti possono venire ritardati in modo diverso da un ripetitore. Infatti il ripetitore non impiega sempre lo stesso numero di bit di preambolo per sincronizzare il suo ricevitore sul clock del trasmettitore. Quindi il numero di bit "persi" nel preambolo da un ripetitore, e che devono da questo essere rigenerati introducendo un ritardo di trasmissione, varia da pacchetto a pacchetto.

Quando si hanno due pacchetti consecutivi e il primo subisce un ritardo maggiore del secondo l'IPG tra i due si riduce.

6.5.2 Round Trip Delay

Per un corretto funzionamento dell'algoritmo CSMA/CD è necessario che la stazione trasmittente si accorga di un'eventuale collisione entro una finestra temporale chiamata *collision window* la quale assicura di rilevare una collisione prima di aver trasmesso completamente il pacchetto più corto. Inoltre il frammento di collisione, costituito dalla somma della parte di pacchetto trasmessa più la sequenza di jamming che viene posta in coda, deve avere una lunghezza inferiore a 576 bit time (57.6 μs, impiegati per la trasmissione degli 8 ottetti di preambolo e di SFD, e dei 64 ottetti del pacchetto di lunghezza minima, 576 bit in totale); ciò significa che l'ultimo bit di jamming deve essere trasmesso entro 575 bit-time (57.5 μs) dall'inizio della trasmissione.

La lunghezza massima del frammento di collisione pone però dei limiti più restrittivi sul tempo di ritardo della rete rispetto a quelli della collision window; infatti, se la collisione venisse rilevata dopo 511 bit time dalla trasmissione dello SFD e quindi la stazione interrompesse la trasmissione per trasmettere la sequenza di jamming, ne risulterebbe un frammento di collisione superiore a 576 bit time.

I frammenti di collisione con lunghezza superiore al massimo consentito non vengono visti come tali dalle stazioni in ascolto, bensì come pacchetti contenenti errori quali *CRC error* o *alignment error*. Se la stazione trasmittente rileva la collisione entro un tempo superiore alla collision window, incrementa il contatore delle *late collision*.

Il tempo di ritardo massimo che può intercorrere da quando la stazione ha trasmesso il primo bit del preambolo a quando viene propagato l'ultimo bit di jamming nel segmento su cui essa è collegata viene chiamato *round trip delay*. Esso non deve essere superiore al massimo frammento di collisione cioè 575 bit time (si veda la figura 6.29). Nel calcolo del round trip delay si considera sempre

una rete di estensione massima, e quindi contenente dei repeater; pertanto si prende in esame la sequenza di jamming del repeater che è di 96 bit, più lunga di quella della stazione che è di 32 bit.

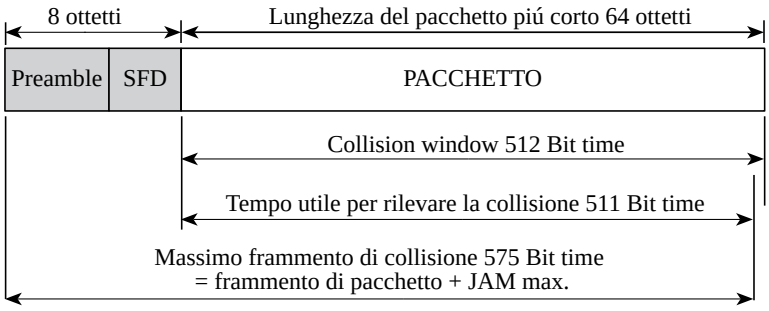

8 ottetti
Lunghezza del pacchetto piú corto 64 ottetti
Preamble
SFD
PACCHETTO
Collision window 512 Bit time
Tempo utile per rilevare la collisione 511 Bit time
Massimo frammento di collisione 575 Bit time
= frammento di pacchetto + JAM max.

Fig. 6.29 - Collision window e massimo frammento di collisione.

Il caso più critico si verifica quando due stazioni sono connesse agli estremi di una LAN con dei ripetitori (figura 6.30) e accadono i seguenti fatti:

- la stazione DTE 1 inizia a trasmettere un pacchetto e questo si propaga verso DTE 2;
- quando il pacchetto è prossimo alla stazione DTE 2 questa inizia a trasmettere;
- avviene una collisione in corrispondenza della stazione DTE 2;
- i bit del pacchetto della stazione DTE 2 che hanno generato la collisione si propagano lungo il segmento 2 e raggiungono il repeater Rep. 1 il quale trasmette una sequenza di 96 bit di jamming sul segmento 1;
- la sequenza di jamming originata dal repeater si sovrappone al pacchetto trasmesso dalla stazione DTE 1, che rileva così la collisione;
- la stazione DTE 1 interrompe la trasmissione del pacchetto e trasmette una sequenza di 32 bit di jamming;
- l'ultimo bit della sequenza di jamming del repeater si propaga lungo il segmento 1, mentre la sequenza di jamming della stazione DTE 1 era terminata prima, in quanto più corta.

Si osservi che l'assimetria nel tempo di propagazione in figura 6.30 è dovuta al fatto che il repeater viene attraversato in un senso dal pacchetto di dato e in senso opposto dalla collisione.

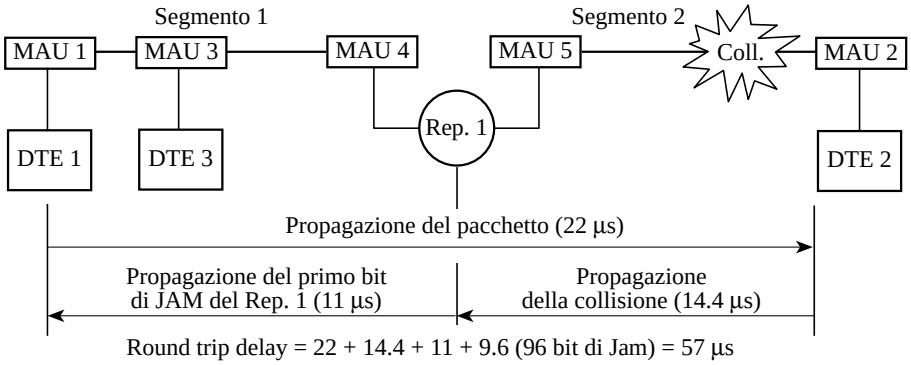


Fig. 6.30 - Round trip delay.

6.6 REGOLE DI CONFIGURAZIONE: PRIMA VERSIONE

Le prime versioni dello standard imponevano regole di configurazione piuttosto restrittive e talvolta imprecise o poco chiare. Questo è dovuto al fatto che l'introduzione di nuovi mezzi trasmissivi ha richiesto l'aggiunta di addendum allo standard originale, con nuove regole di configurazione. Tali regole sono qui riportate, in quanto ampiamente usate dai progettisti di LAN, anche se sconsigliate in quanto ormai superate dalla nuova versione.

Si definiscono due tipi di segmenti:

- segmento di tipo *coax* che può essere 10Base5 o 10Base2;
- segmento di tipo *link* che può essere FOIRL o 10BaseT.

Sono fissati i seguenti limiti al numero massimo di ripetitori e di segmenti che si possono avere in un percorso tra due stazioni:

- 4 ripetitori;
- 5 segmenti, di cui al massimo 3 coax;
- se si hanno 4 ripetitori, ogni singolo segmento FOIRL non deve eccedere i 500 m;
- se si hanno 3 ripetitori, ogni singolo segmento FOIRL non deve eccedere i 1000 m.

La presenza dei ripetitori connessi a diversi tipi di segmenti può ridurre in modo diverso l'IPG, e comunque, se si rispettano le regole sopra riportate, sebbene siano un po' restrittive, non si verificano problemi di IPG troppo corto o di round trip delay eccessivo.

La figura 6.31 mostra un esempio di configurazione massima con 4 ripetitori in cui i segmenti di FOIRL devono essere limitati a 500 m.

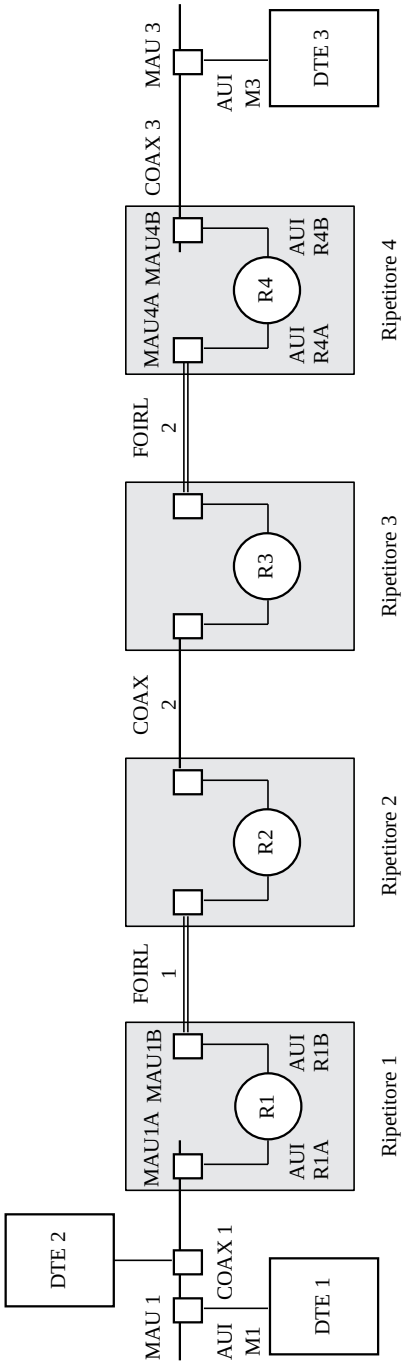


Fig. 6.31 - Interconnessione FOIRL.

La figura 6.32 mostra un esempio con quattro ripetitori in cui i segmenti di tipo link utilizzati per interconnettere le stazioni sono 10BaseT.

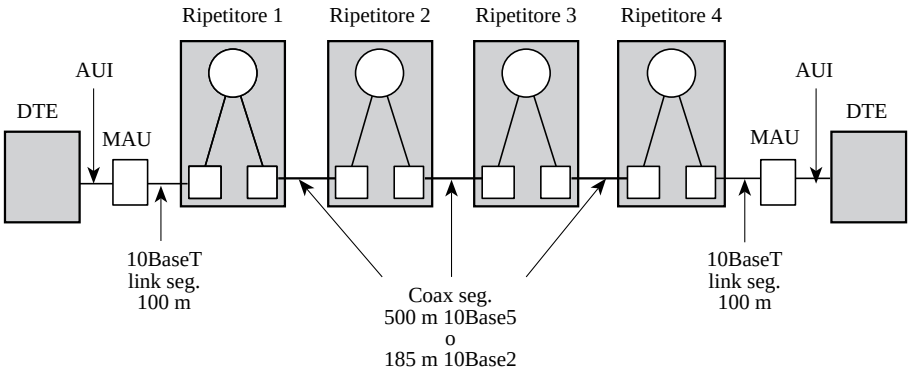


Fig. 6.32 - Esempio di configurazione massima n. 2.

La figura 6.33 mostra un altro esempio con quattro ripetitori e segmenti link sia di tipo FOIRL (massimo 500 m) sia di tipo 10BaseT.

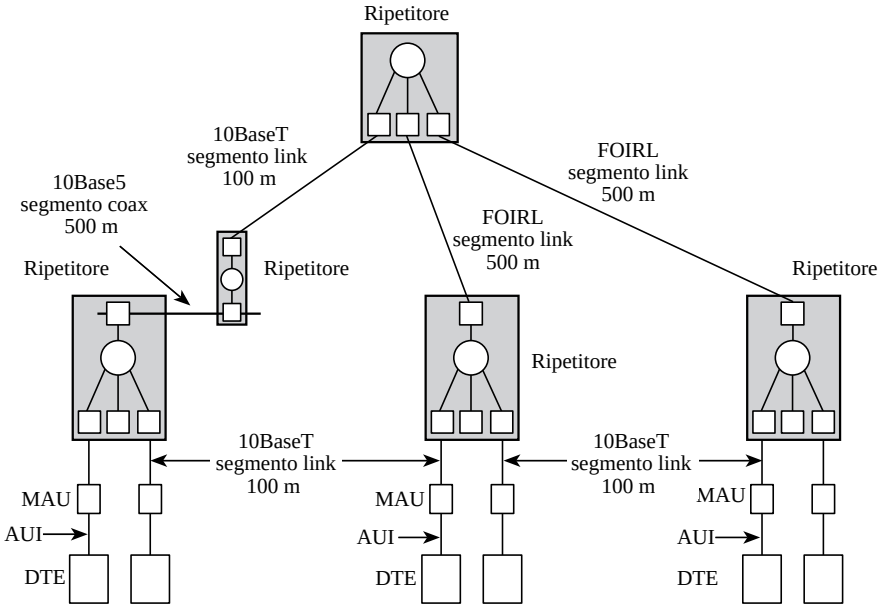


Fig. 6.33 - Esempio di configurazione massima n. 3.

La figura 6.34 mostra un esempio con tre soli ripetitori in cui i segmenti FOIRL possono raggiungere la lunghezza di 1000 m.

Infine, la figura 6.35 mostra un esempio di configurazione non valida in quanto, pur avendo solo 3 ripetitori in cascata, il cammino tra le stazioni A e B ha 4 segmenti di tipo coax.

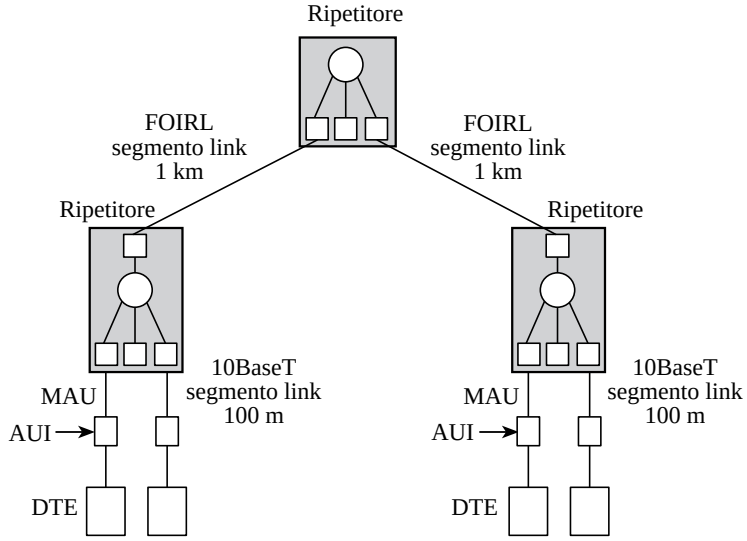


Fig. 6.34 - Esempio di configurazione massima n. 4.

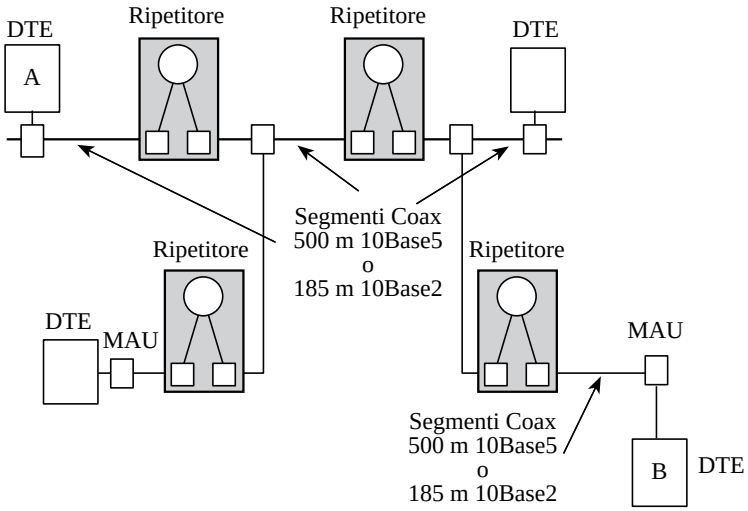


Fig. 6.35 - Esempio di configurazione non valida.

6.7 REGOLE DI CONFIGURAZIONE: SECONDA VERSIONE

Queste regole sono tratte dalla quarta edizione dello standard datata 8/7/1993. I parametri da considerare sono i seguenti:

- la lunghezza dei segmenti ed i ritardi di propagazione ad essi associati;
- i ritardi associati a ciascuna *repeater unit*, cioè all'insieme di un ripetitore, dei transceiver ad esso collegati e dei cavi AUI (detto nel seguito ripetitore per semplicità);
- il ritardo associato ai MAU delle stazioni;
- il ritardo del DTE associato al metodo di accesso CSMA/CD;
- la riduzione dell'IPG dovuta ai ripetitori.

6.7.1 Definizioni

Il termine *link segment* indica una connessione punto-punto tra due transceiver FOIRL, 10BaseT, 10BaseFB o 10BaseFL.

Il termine *mixing segment* indica un segmento in grado di interconnettere più di 2 transceiver di tipo 10Base5, 10Base2 o 10BaseFP.

Il *path* è il percorso tra due DTE che attraversa segmenti, ripetitore, MAU.

Il *Segment Delay Value (SDV)* è il ritardo di un dato segmento; comprende sempre anche il ritardo introdotto dal ripetitore.

Il *Segment Variability Value (SVV)* è un numero associato ad un dato segmento, incluso un ripetitore, che rappresenta la variabilità del ritardo, ovvero l'entità di riduzione dell'IPG per quel segmento.

Il *Path Delay Value (PDV)* è la somma di tutti i SDV riferiti ai segmenti che costituiscono un percorso tra due DTE.

Il *Path Variabilty Value (PVV)* è la somma di tutti i SVV riferiti ai segmenti che costituiscono un percorso tra due DTE.

Un segmento 10BaseFP è composto da due qualunque link in fibra ottica più la stella passiva che li interconnette, quando presente.

6.7.2 Parametri associati ai segmenti

La tabella 6.3 riporta per i vari tipi di segmenti la massima lunghezza ammessa, il massimo numero di transceiver collegabili, la minima velocità di propagazione ammessa e il ritardo massimo introdotto.

Tipo di segmento	Max. num. di MAU per segm.	Lungh. max. segm.	Velocità min. di propagaz.	Ritardo max. per segm. (ns)
Mixing segment				
10Base5	100	500	0.77 c[1]	2165
10Base2	30	185	0.65 c	950
10BaseFP	33[3]	1000[2]	0.66 c	5000
Link segment				
FOIRL	2	1000	0.66 c	5000
10BaseT[4]	2	100	0.59 c	565
10BaseFB	2	2000	0.66 c	10000
10BaseFL	2	2000	0.66 c	10000

1 - c = 3 x 10^8 m/s (velocità della luce nel vuoto)
2 - la connessione MAU-to-star non deve superare i 500 m
3 - il numero di MAU dipende dalle caratteristiche della star passiva
4 - la lunghezza max. del segmento dipende dalle caratteristiche del cavo

Tab. 6.3 - Parametri associati ai segmenti.

6.7.3 Primo modello di configurazione

Questo modello ha delle regole semplici, ma un po' restrittive:

- il numero massimo di ripetitori ammesso in un percorso tra due stazioni è 4;
- il numero massimo di segmenti è 5, di cui 3 possono essere mixing segment;
- i cavi AUI per i MAU 10BaseFP e 10BaseFL non devono eccedere i 25 m;
- quando in un path sono presenti 5 segmenti in fibra ottica:
  - i segmenti FOIRL, 10BaseFB e 10BaseFL non possono superare i 500 m;
  - il segmento più lungo 10BaseFP non deve eccedere i 300 m;
- quando sono presenti 4 segmenti e 3 ripetitori in un path:
  - ogni segmento inter-repeater in fibra ottica non deve eccedere i 1000 m se riferito a un link di tipo FOIRL, 10BaseFB o 10BaseFL e i 700 m se il segmento è di tipo 10BaseFP;
  - la lunghezza massima di un segmento di fibra ottica che interconnette una stazione ad un ripetitore non deve superare i 400 m nel caso 10BaseFL e 300 m nel caso 10BaseFP.

La figura 6.36 mostra un esempio di configurazione che comprende una stella ottica passiva con tre ripetitori.

La figura 6.37 mostra la stessa configurazione di figura 6.36 con l'aggiunta di un quarto ripetitore e la conseguente riduzione delle lunghezze dei segmenti in fibra ottica.

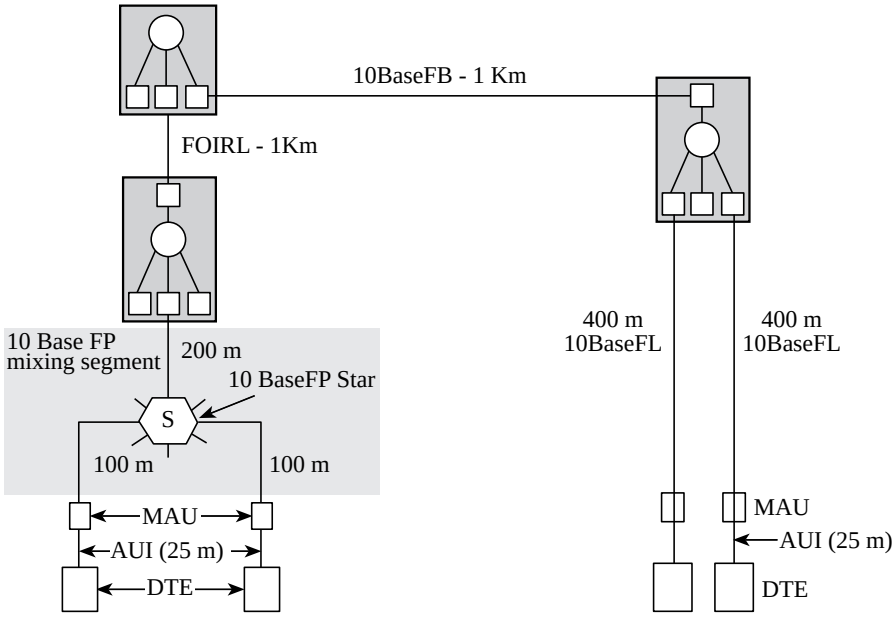


Fig. 6.36 - Esempio di configurazione massima n. 5.

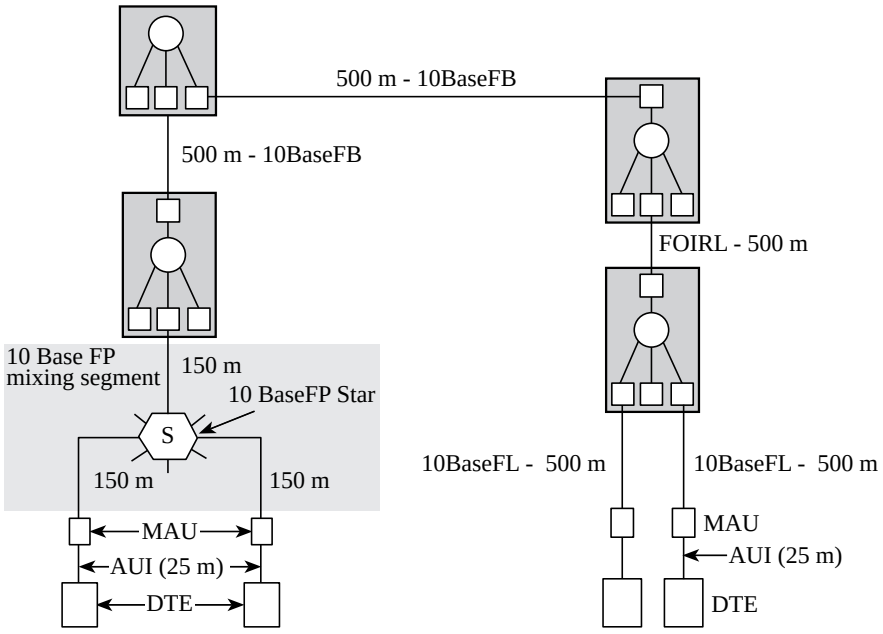


Fig. 6.37 - Esempio di configurazione massima n. 6.

6.7.4 Secondo modello di configurazione

Questo modello permette numerose configurazioni che devono essere dimensionate utilizzando il modello mostrato in figura 6.38.

Il modello si basa sui seguenti presupposti:

- il DTE 1 deve percepire la collisione entro la collision window;
- il round trip delay non deve essere superiore al massimo frammento di collisione, cioè 575 bit time (si veda il paragrafo 6.5.2);
- la variabilità di sincronizzazione sul preambolo introdotta dai ripetitori deve garantire un IPG minimo di 47 bit time (4.7 μs).

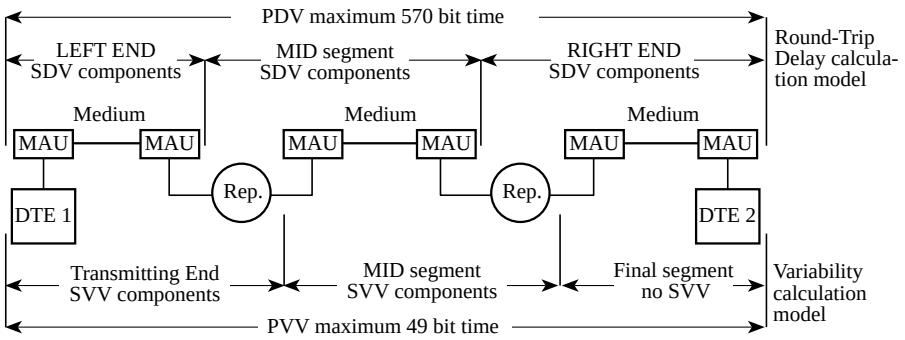


Fig. 6.38 - Modello di riferimento per il calcolo.

Prima regola di configurazione:

- il caso peggiore per il PDV non deve superare 570 bit time (575 bit - 5 bit di margine di sicurezza);
- il PDV è la somma di tutti i SDV associati ai segmenti che compongono un path; nella somma devono essere inclusi anche gli eventuali cavi AUI;
- per determinare il valore di SDV bisogna considerare i valori dei parametri riportati nella tabella 6.4 ed utilizzare la seguente formula:

$$SDV = base + [length \cdot (round\ trip\ delay/meter)]$$

I valori riportati nella tabella 6.4 sono mediati ed hanno il seguente significato:

- *Base* è il valore base di ogni segmento e indica la somma dei ritardi dei vari componenti attivi (DTE, MAU, ripetitore) più 2 m per ogni cavo AUI connesso ai MAU presenti nel percorso;

- *Max* è il valore massimo ed è il risultato della somma del valore base più il ritardo inserito dal segmento di lunghezza massima.
- *Round trip delay/meter* è l'incremento di ritardo introdotto da ogni metro di cavo o fibra.

Qualora i cavi AUI abbiano lunghezze maggiori di 2 m, bisogna aggiungere il ritardo dell'eccedenza di cavo AUI per ogni SDV. In pratica si aggiunge spesso tutta la lunghezza del cavo AUI e non solo l'eccedenza, poiché la differenza è minima ed il risultato finale è più restrittivo e quindi più sicuro.

Round-trip delay values in Bit time (PDV max. 570)								
Segment type	Max. lenght	Left end		Mid-segment		Right end		RT delay/meter
		Base	Max.	Base	Max.	Base	Max.	
10Base5 coax	500	11.75	55.05	46.5	89.8	169.5	212.8	0.0866
10Base2 coax	185	11.75	30.731	46.5	65.48	169.5	188.48	0.1026
FOIRL	1000	7.75	107.75	29	129	152	252	0.1
10BaseT	100*	15.25	26.55	42	53.3	165	176.3	0.113
10BaseFP	1000	11.25	111.25	61	161	183.5	284	0.1
10Base FB	2000	N/A**	N/A**	24	224	N/A**	N/A***	0.1
10BaseFL	2000	12.25	212.25	33.5	233.5	156.5	365.5	0.1
Excess lenght AUI	48	0	4.88	0	4.88	0	4.88	0.1026

* La lunghezza massima del segmento dipende dalle caratteristiche del cavo.
** N/A non applicabile poiché il 10BaseFB non supporta la end-connection.

Tab. 6.4 - Path Delay Value.

Esempio di calcolo

Prendiamo la figura 6.38 e supponiamo che il segmento a cui è connesso DTE 1 sia un coassiale 10Base5 lungo 350 m, supponiamo poi che il MID segment sia un link da 800 m di tipo FOIRL e che il segmento connesso al DTE 2 sia un cavo UTP da 50 m; supponiamo inoltre che i due DTE siano connessi tramite cavi AUI da 20 m.

Consideriamo prima come left end il segmento DTE 1 e come right end il segmento DTE 2.

SDV Left end = 11.75 + [350 · 0.0866] + 20 · 0.1026 = 44.11
SDV MID seg. = 29 + [800 · 0.1] = 29 + 80 = 109
SDV Right end = 165 + [50 · 0.113] + 20 · 0.1026 =172.7
PDV = 44.11 + 109 + 172.70 = 325.81 bit time

Consideriamo ora come left end il segmento DTE 2 e come right end il segmento DTE 1; non ricalcoliamo più il MID segment poiché il valore di SDV rimane invariato.

SDV Left end = 15.25 + [50 · 0.113] + 20 · 0.1026 = 22.95
SDV Right end = 169.5 + [350 · 0.0866] + 20 · 0.1026 = 201.86
PDV = 22.95 + 109 + 201.86 = 333.81 bit time

Tra i due casi di calcolo bisogna considerare il caso peggiore e quindi il PDV dell'esempio sarà 333.81 bit time.

Seconda regola di configurazione:

Per evitare che il valore di valore dell'IPG scenda al di sotto dei limiti accettabili è necessario che il valore di PVV nel caso peggiore sia inferiore a 49 bit time.

Il PVV è la somma di tutti i valori di SVV, e il valore di SVV si determina tramite la tabella 6.5.

Segment variability values in bit time (PVV max 49)		
Segment type	Transmitting end	Mid-segment
Coax	16	11
Link except 10BaseFB	10.5	8
10BaseFB	N/A**	2
10BaseFP	11	8

** N/A non applicabile poiché il 10BaseFB non supporta le end-connection

Tab. 6.5 - Segment Variability Value.

Riprendiamo il precedente esempio e calcoliamo il PVV.

Consideriamo prima come transmitting end il segmento DTE 1.

PVV = 16 + 8 = 24 bit time.

Consideriamo ora come transmitting end il segmento DTE 2.

PVV = 10.5 + 8 = 18.5 bit time.

Il valore di PVV da considerare deve essere quello peggiore e quindi il PVV dell'esempio sarà 24 bit time.

Una configurazione è valida quando entrambe le regole di configurazione sono rispettate e quindi quando il caso peggiore di PDV è inferiore a 570 bit time ed il caso peggiore di PVV è inferiore a 49 bit time.

6.8 CONVIVENZA DI ETHERNET E IEEE 802.3

Sino a questo punto le reti locali Ethernet v.2.0 e IEEE 802.3 sono state descritte come delle realtà simili, ma distinte. In pratica è però molto comune trovare delle reti miste ed in particolare è oggi molto diffusa la situazione in cui l'hardware è conforme al più recente standard IEEE 802.3, ma il formato dei pacchetti continua ad essere quello di Ethernet v.2.0.

Questo non crea alcun problema alle schede poiché in fase di ricezione si è comunque in grado di distinguere i due tipi di pacchetti.

Per meglio comprenderere questo punto consideriamo come i protocolli di livello superiore si appoggiano sulle due reti locali (figura 6.39).

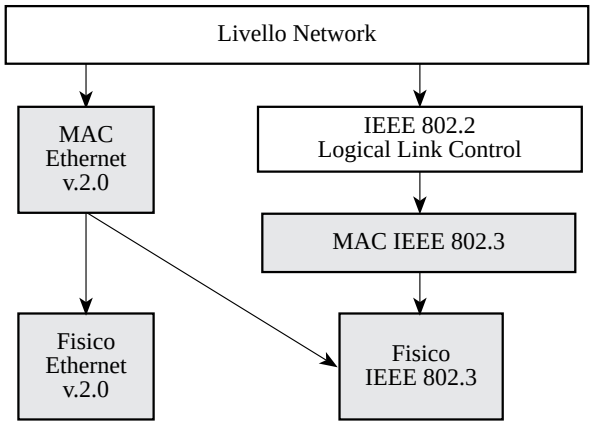


Fig. 6.39 - Pile di protocolli Ethernet e 802.3.

Come risulta evidente dalla figura, nel caso di Ethernet la PDU di livello 3 è contenuta direttamente nel pacchetto MAC, mentre nel caso 802.3 la PDU di livello 3 è contenuta nella PDU di livello LLC e quest'ultima è contenuta nel campo dati MAC.

Esempi di tali imbustamenti sono presenti in appendice B; in B.5 è riportato un imbustamento Ethernet e in B.7 un imbustamento 802.3.

Per capire come una scheda di rete locale discrimina in fase di ricezione i pacchetti Ethernet da quelli 802.3 si analizzi la figura 6.40 che mostra entrambi i pacchetti. Il primo campo diverso è quello lungo 2 byte che in Ethernet assume il significato di protocol type e in 802.3 quello di length. Gli insiemi di valori ammissibili nei due casi sono disgiunti, come appare anche evidente dall'appendice A, paragrafo A.2. Infatti, in 802.3 il campo length può assumere valori nell'intervallo 0-1500, mentre le codifiche di protocol type in Ethernet sono tutte maggiori o uguali a 1536.

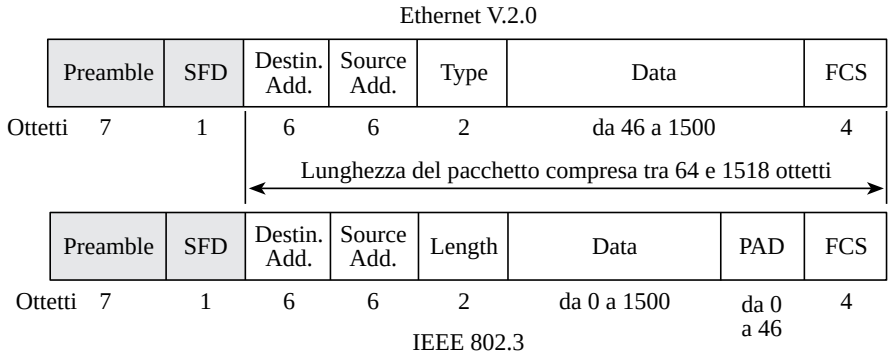


Fig. 6.40 - Pacchetti Ethernet e 802.3.

Quindi una scheda durante la ricezione di un pacchetto verifica il contenuto di quei due byte:

- se il contenuto è superiore a 1500 si tratta di un pacchetto Ethernet e il contenuto è il protocol type, e quindi si può direttamente passare il pacchetto al livello 3 corrispondente;
- se il contenuto è minore o uguale a 1500 allora si tratta di un pacchetto 802.3 e il contenuto è la length del campo dati. Il tipo di protocollo di livello 3 è contenuto in questo caso nella busta LLC, eventualmente di tipo SNAP, in accordo con quanto descritto nel paragrafo 5.7.4.

BIBLIOGRAFIA

[1] "The Ethernet. A Local Area Network Data Link Layer and Physical Layer Specification," Version 2.0, November 1982, document no. AA-K759B-TK, Digital Equipment Corporation Maynard (MA), Intel Corporation Santa Clara (CA), Xerox Corporation Stamford (Ca).

[2] ISO/IEC 8802.3, ANSI/IEEE Std 802.3 fourth edition 1993-07-08, Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and physical layer specifications.

[3] IEEE Std 802.3j-1993 Supplemento Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and physical layer specifications. Fiber Optic Active and Passive Star-Based Segment, type 10BASE-F (Sections 15-18).

7

LA RETE TOKEN RING E LO STANDARD IEEE 802.5

7.1 INTRODUZIONE

Token Ring nasce nei laboratori IBM nel 1976, come rete locale alternativa a Ethernet. Essa è concepita per operare su un cablaggio a stella, realizzato con cavo STP di tipo 1. La prima versione ha una velocità trasmissiva di 4 Mb/s.

Nel 1982 la IEEE crea il comitato IEEE 802.5, che ha lo scopo di redigere uno standard per Token Ring relativamente al livello 1 ed al sottolivello MAC del livello 2 (figura 7.1). Il comitato apporta alcune modifiche e introduce anche una versione a 16 Mb/s che utilizza concentratori passivi e cavi di tipo STP.

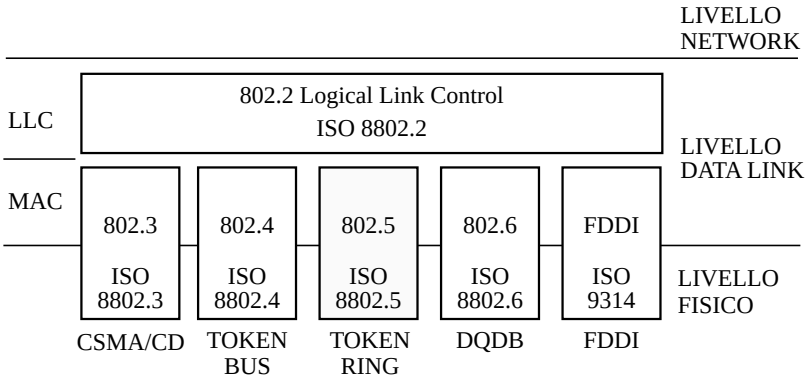


Fig. 7.1 - Il progetto IEEE 802.

Nel 1985 lo standard IEEE 802.5 viene adottato dal comitato 97 dell'ISO come ISO/DIS 8802.5 (Draft International Standard) e nel 1992 viene approvato come

standard ISO 8802.5.

Nel 1993 il comitato IEEE pubblica una bozza chiamata 802.5 Q/Draft 3 che espone in modo più chiaro e dettagliato diversi aspetti dello standard pubblicato precedentemente. In particolare, la bozza migliora alcuni aspetti del livello MAC, introduce la possibilità di utilizzare i cavi UTP e definisce nuovi concentratori di tipo attivo o parzialmente attivo.

Questa pluralità di standard introduce una certa confusione su cosa sia Token Ring, come funzioni e quali siano le regole di configurazione. Occorre tuttavia sottolineare che i costruttori di apparati si stanno adeguando rapidamente all'ultima versione del 1993, sebbene non sia stata ancora approvata come standard, in quanto risulta essere molto più flessibile e funzionale rispetto alle precedenti.

Nei successivi paragrafi si cercherà di fare chiarezza su tali problematiche, trattando in ordine il MAC, il livello Fisico e le regole di configurazione.

7.2 METODO DI ACCESSO A TOKEN

Una rete Token Ring consiste in un certo numero di stazioni collegate serialmente tramite un mezzo trasmissivo e richiuse ad anello. I pacchetti vengono trasferiti da una stazione ad un'altra serialmente; ogni stazione ripete e rigenera la trasmissione verso la stazione successiva.

Poiché le stazioni devono ripetere continuamente i pacchetti delle altre stazioni, per ragioni di affidabilità la rete viene cablata a stella, come spiegato nel paragrafo 3.5.2.

I collegamenti tra il centro stella e le stazioni prendono il nome di "lobi". Quando una stazione è spenta o guasta, il centro stella (concentratore) la esclude dalla rete (figura 7.2).

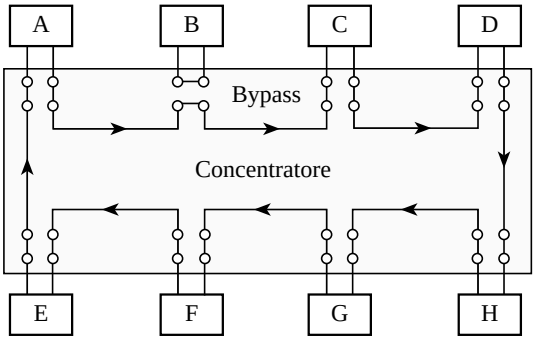


Fig. 7.2 - Schema logico di una rete Token Ring.

Il metodo di accesso (MAC) è di tipo a token. Il token (gettone) è un particolare pacchetto che circola sull'anello (ring), indicando che l'anello è libero. Una stazione che intenda trasmettere deve aspettare che arrivi il token, catturarlo e quindi trasmettere.

Il token circola continuamente sull'anello anche se le stazioni non hanno dati da trasmettere. Esso viene generato inizialmente dalla stazione che si è guadagnata il diritto di essere *l'active monitor* della rete e viene ripetuto da tutte le stazioni.

Quando una stazione cattura il token essa può trasmettere uno o più pacchetti, in funzione della loro lunghezza e di un parametro detto THT (*Timer Holding Token*) che indica il tempo massimo per cui una stazione può trattenere il token.

7.2.1 Formato del token e del pacchetto

La figura 7.3 mostra il formato del token e del pacchetto 802.5.

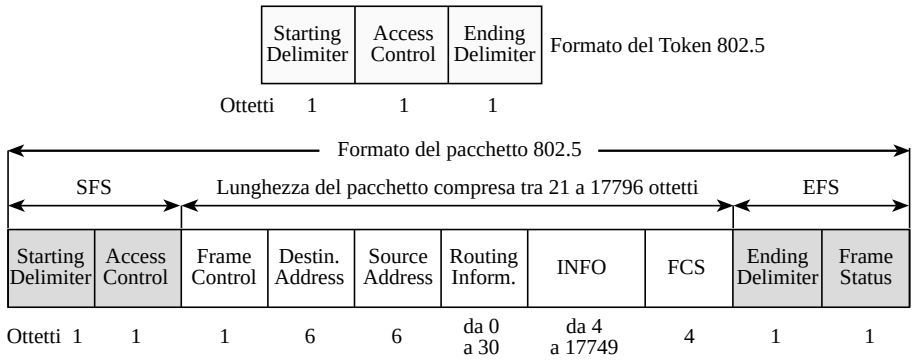


Fig. 7.3 - Formato del token e del pacchetto.

Il token è formato da 3 ottetti (24 bit): lo starting delimiter, l'access control, l'end delimiter. Questi tre campi hanno formato e funzioni analoghe per il token e per il pacchetto (figura 7.4).

Il pacchetto è delimitato da due sequenze:

- la *Start-of-Frame Sequence* (SFS) che indica l'inizio del pacchetto ed è formata da un ottetto di starting delimiter e da un secondo ottetto di access control;
- la *End-of-Frame Sequence* (EFS) che indica la fine di un pacchetto ed è formata da un ottetto di ending delimiter e da un secondo ottetto di frame status.

Il campo *Starting Delimiter* (SD) identifica in modo univoco l'inizio del token o del pacchetto. A tal fine, esso contiene dei bit identificati con J e K che violano il codice di Manchester.

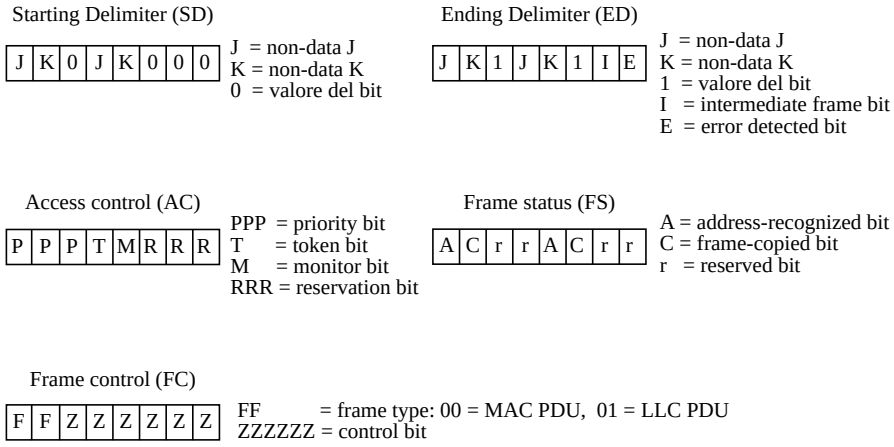

Starting Delimiter (SD)
J K 0 J K 0 0 0
J = non-data J
K = non-data K
0 = valore del bit
Ending Delimiter (ED)
J K 1 J K 1 I E
J = non-data J
K = non-data K
1 = valore del bit
I = intermediate frame bit
E = error detected bit
Access control (AC)
P P P T M R R R
PPP = priority bit
T = token bit
M = monitor bit
RRR = reservation bit
Frame status (FS)
A C r r A C r r
A = address-recognized bit
C = frame-copied bit
r = reserved bit
Frame control (FC)
F F Z Z Z Z Z Z
FF = frame type: 00 = MAC PDU, 01 = LLC PDU
ZZZZZZ = control bit

Fig. 7.4 - Formato di alcuni campi del pacchetto o del token.

Il campo *Access Control* (AC) contiene le informazioni di accesso al ring. Il *token bit* assume valore 0 nel caso del token e valore 1 nel caso di un pacchetto. I *reservation bit* indicano la priorità d'accesso richiesta. I *priority bit* indicano la priorità d'accesso attuale.

Il campo di *Ending Delimiter* (ED) indica la fine del pacchetto.

L'ottetto *Frame Status* (FS) contiene i bit di *address-recognized* (A) e *frame-copied* (C). Le combinazioni di questi due bit indicano che:

- la stazione è inesistente o inattiva nel ring (A=0, C=0);
- la stazione esiste, ma il pacchetto non è stato copiato (A=1, C=0);
- il pacchetto è stato copiato (A=1; C=1).

Il pacchetto vero e proprio inizia dopo la SFS e può avere una lunghezza compresa tra 21 e 17796 ottetti, di cui al massimo 17749 per il campo dati (INFO).

Nel campo *Destination Address* (DA) è contenuto l'indirizzo della stazione a cui è destinato il pacchetto, nel campo *Source Address* (SA) è contenuto l'indirizzo della stazione che ha generato il pacchetto.

Il campo *Routing Information* (RI) contiene le informazioni d'instradamento del pacchetto attraverso una rete locale estesa (si veda il paragrafo 10.20.1).

Il campo *Frame Control* (FC) definisce il contenuto del pacchetto: se il valore dei bit FF è 00 allora il pacchetto è una trama MAC (usata per scopi di management) che

deve essere ricevuta da tutte le stazioni (ad esempio, *beaconing frame* o *ring purge*; si vedano i paragrafi 7.2.8 e 7.2.10), se il valore è 01 allora il pacchetto contiene una LLC-PDU.

Il campo *Frame Check Sequence* (FCS) contiene il CRC calcolata sui campi descritti precedentemente.

7.2.2 Architettura di una stazione Token Ring

La figura 7.5 mostra l'architettura di una stazione Token Ring. Si noti il *repeat path* che è il cammino usato per ripetere i pacchetti ed è inserito direttamente tra ring-in e ring-out. I simboli ricevuti vengono anche passati al livello superiore.

Quando la stazione deve trasmettere essa stessa un pacchetto, disabilita il repeat path e preleva i simboli dal livello superiore.

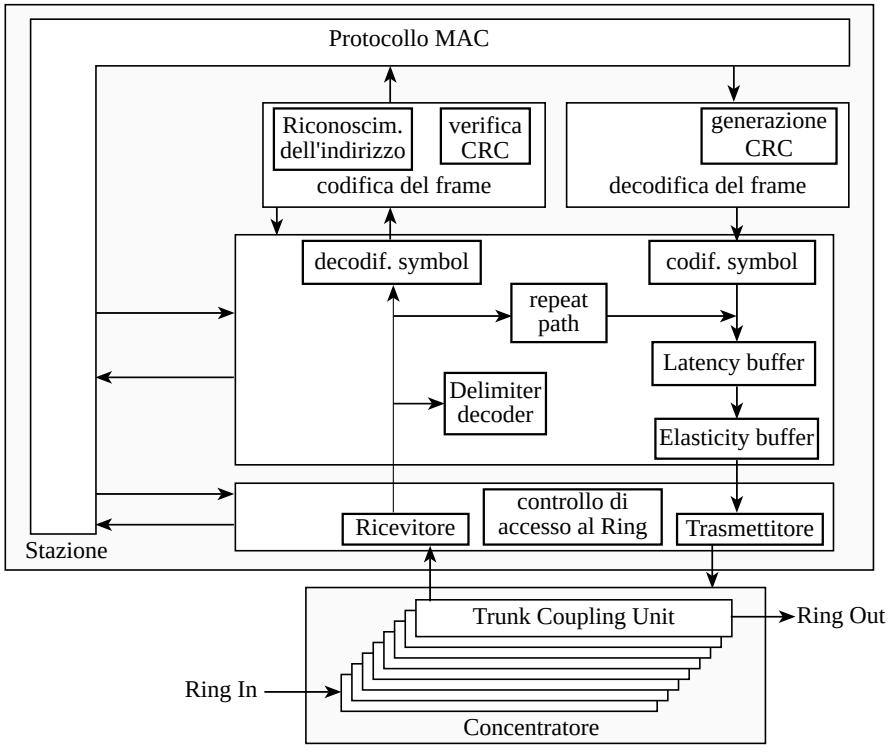


Fig. 7.5 - Architettura di una stazione 802.5.

7.2.3 Trasmissione, ripetizione e ricezione dei pacchetti

La trasmissione di un pacchetto dalla stazione A alla stazione C (figura 7.6) avviene nel seguente modo:

- A attende di ricevere il token dal ring-in e lo cattura. L'operazione di cattura avviene portando a 1 il *token-bit* del campo Access-Control (AC). Tale modifica trasforma il token in un pacchetto ed in particolare la parte già ritrasmessa sul ring-out diviene la Start-of-Frame Sequence (SFS);

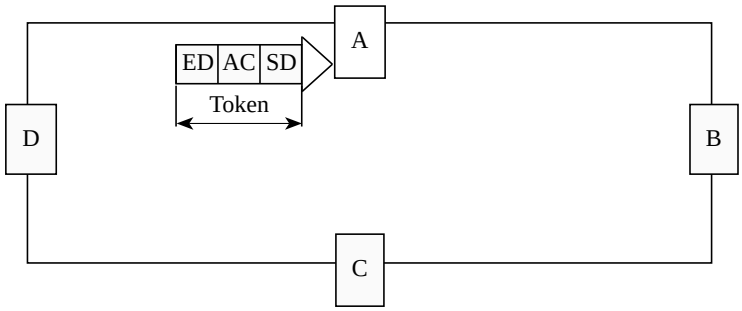


Fig. 7.6 - Trasmissione: fase 1.

- la stazione A inibisce il circuito di ripetizione dei bit (repeat path) tra ring-in e ring-out;
- la stazione A trasmette il Frame Control (FC), l'indirizzo di destinazione (DA), l'indirizzo di mittente (SA) ed eventualmente delle informazioni per i bridge source routing (RI);
- la stazione A trasferisce i dati nel campo INFO (figura 7.7);

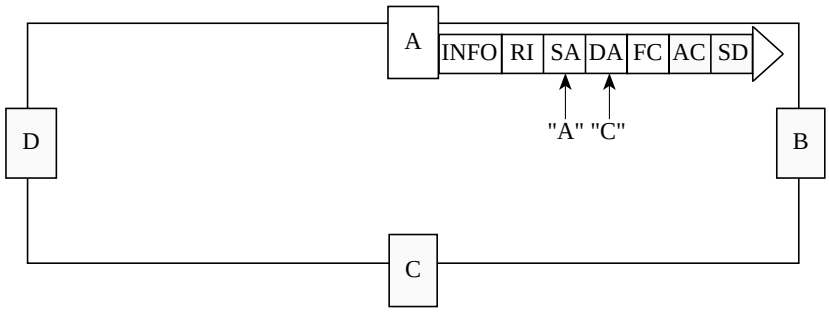


Fig. 7.7 - Trasmissione: fase 2.

- se la stazione A ha altri pacchetti da trasmettere e non ha ancora superato il THT, allora mette a uno l'*intermediate bit* dell'End Delimiter (ED) ed inizia la trasmissione del pacchetto successivo;
- quando la stazione A ha trasmesso l'ultimo pacchetto mette a zero l'intermediate bit dell'end delimiter;
- se A termina la trasmissione di un pacchetto prima di aver iniziato a riceverlo indietro da ring-in (la rete è ad anello), trasmette dei bit di riempimento (fill) su ring-out fino a quando non può generare il nuovo token;
- quando A riceve sulla porta di ring-in il campo di Source Address (SA) del pacchetto trasmesso (figura 7.8) e lo riconosce come proprio, toglie il pacchetto dall'anello e si predispone per emettere il token. Se la trasmissione dei pacchetti è terminata, genera immediatamente il nuovo token, in caso contrario attende il termine della trasmissione.

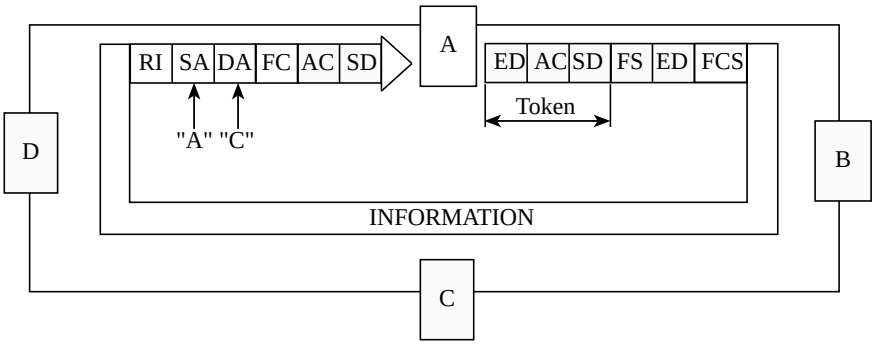


Fig. 7.8 - Generazione del nuovo token.

Tutte le stazioni che non hanno il possesso del token (in questo caso B, C e D) ripetono i bit che ricevono verso la stazione successiva. Se durante tale operazione verificano la presenza di errori, li evidenziano modificando in modo opportuno il bit E dell'Ending Delimiter.

Ogni stazione osserva i pacchetti che ripete per verificare se l'indirizzo di destinazione (DA) è uguale al proprio indirizzo MAC (figura 7.9). Tale uguaglianza si verifica unicamente sulla stazione cui è destinato il pacchetto. Essa, oltre a continuare a ripetere il pacchetto, ne effettua la ricezione e modifica in modo opportuno l'*address recognized bit* e il *copied bit*, nel campo Frame Status (FS).

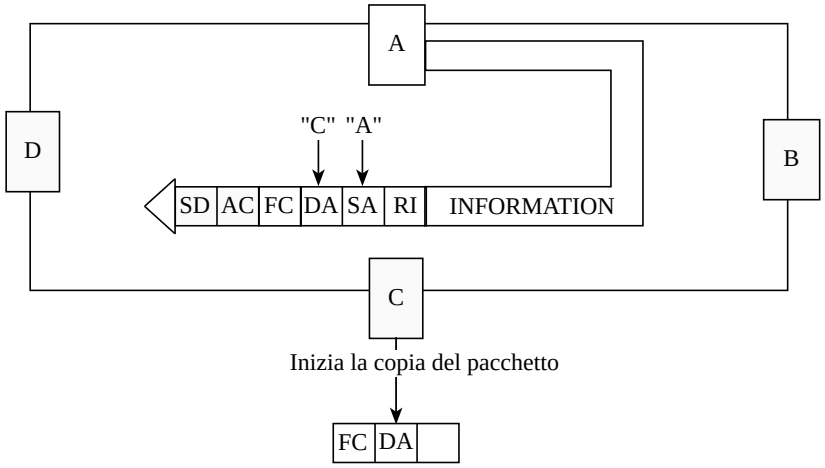


Fig. 7.9 - Ricezione del pacchetto.

Alla fine della ricezione dei propri pacchetti (figura 7.10), la stazione A riabilita la ripetizione dei bit ricevuti (circuito di repeat path) tra la porta di ring-in e quella di ring-out.

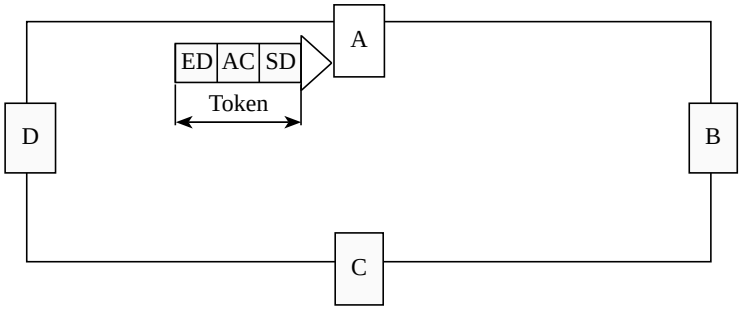


Fig. 7.10 - Riabilitazione della ripetizione.

7.2.4 Lunghezza massima dei pacchetti

La lunghezza massima del pacchetto, includendo i campi SFS e EFS, dipende dalla velocità trasmissiva e dal valore di THT (Timer Holding Token) che può essere al massimo di 8.9 ms.

Considerando che:

- a 4 Mb/s il tempo di trasmissione di un bit è di 250 ns;

- a 16 Mb/s il tempo di trasmissione di un bit è di 62,5 ns;

il risultato che si ottiene è il seguente:

- a 4 Mb/s la lunghezza massima del pacchetto è uguale a: $\frac{8.9 \cdot 10^{-3}}{250 \cdot 10^{-9} \cdot 8} = 4450$ ottetti;
- a 16 Mb/s la lunghezza massima del pacchetto è uguale a: $\frac{8.9 \cdot 10^{-3}}{62.5 \cdot 10^{-9} \cdot 8} = 17800$ ottetti.

7.2.5 Sincronizzazione

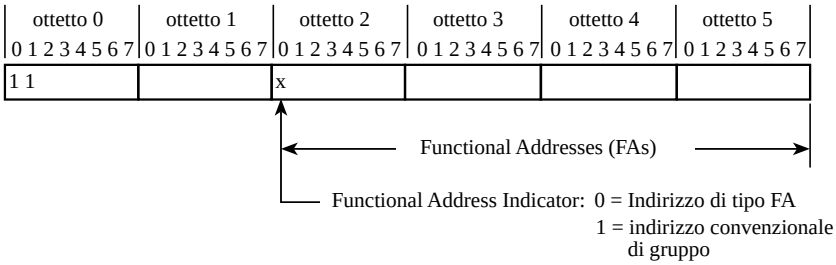
I pacchetti e i token sono normalmente consecutivi, cioè sono trasmessi in sequenza. In questo caso la sincronizzazione è mantenuta permanentemente tra le stazioni. Tuttavia, la presenza di guasti può far sì che le stazioni si desincronizzino a causa dell'assenza di trasmissione. Per ovviare a tale situazione il primo pacchetto o token di una sequenza è preceduto da un gruppo di 20 bit (una sorta di preambolo) che serve alla stazione ricevente per sincronizzare il proprio clock interno.

7.2.6 Indirizzi funzionali

Ci sono alcuni indirizzi MAC di multicast, amministrati localmente, che vengono detti indirizzi funzionali (*functional addresses*). Essi si servono a realizzare le seguenti quattro funzioni:

- *active monitor* è la funzione svolta dalla stazione che genera il token, stabilisce il clock di riferimento per tutte le altre stazioni, genera il processo periodico di notifica di vicinanza della stazione, recupera condizioni di token perso;
- *ring parameter server* è la funzione responsabile di inizializzare un gruppo di parametri relativi alle stazioni attive nel ring;
- *ring error monitor* è la funzione che colleziona gli errori delle stazioni, può inoltre analizzarli e registrarne le statistiche;
- *configuration report server* è la funzione che riceve le informazioni di configurazione dalle stazioni e le inoltra al network manager e, quando questo lo richiede, può verificare le configurazioni e cambiarle, oppure rimuovere una stazione dal ring.

La figura 7.11 mostra la rappresentazione degli indirizzi funzionali secondo la sintassi nativa IEEE 802.5 (*native order*, si veda il paragrafo 5.6.7).



Funzione	Functional Address
Active monitor	C0 00 00 00 00 01
Ring Parameter Server (RPS)	C0 00 00 00 00 02
Ring Error Monitor (REM)	C0 00 00 00 00 08
Ring Configuration Server (RCS)	C0 00 00 00 00 10

Fig. 7.11 - Indirizzi funzionali.

7.2.7 Elezione dell'active monitor

In un anello c'è una sola stazione che svolge funzioni di active monitor per la rete e viene designata per questa funzione a seguito di un processo di elezione (*token claim*). Le altre stazioni si mettono in uno stato di attesa (*standby monitor state*) pronte a diventare l'active monitor della rete nel caso di problemi all'active monitor.

Durante la fase di elezione tutte le stazioni che rilevano l'assenza dell'active monitor trasmettono continuamente dei pacchetti di claim attraverso cui propongono il proprio valore di claim (valore determinato dall'indirizzo della stazione) e controllano i pacchetti ricevuti; comparano quindi la proposta di claim ricevuta con il proprio valore proposto. Se una stazione riceve una proposta di claim superiore al proprio valore interrompe la generazione dei pacchetti di claim e ripete quelli ricevuti, se la proposta ricevuta è inferiore continua a generare i pacchetti di claim. Alla fine una sola stazione riceve il proprio pacchetto di claim ed è quella vincente che diventa l'active monitor.

Essa trasmette prima un pacchetto di azzeramento (*ring purge*) per ripulire il ring e poi genera un nuovo token.

L'active monitor comunica periodicamente la sua presenza a tutte le altre stazioni tramite un pacchetto AMP (*Active Monitor Presence*). Se una stazione in stato di standby monitor non vede transitare un pacchetto AMP per un tempo superiore a TSM (*Timer Standby Monitor*) essa inizia un processo di elezione di un nuovo active monitor.

7.2.8 Azzeramento del ring (ring purge)

Ogni stazione ha un *Timer Valid Transmission* (TVX) che indica il tempo massimo in cui deve avvenire una trasmissione di pacchetti e la conseguente generazione del nuovo token. Questo parametro è usato dall'active monitor per rilevare trasmissioni erroneamente lunghe o l'assenza del token.

Quando scade il TVX, l'active monitor trasmette dei pacchetti di azzeramento dell'anello (ring purge) ed incrementa il contatore di token-error usato per fini statistici. Se riceve un pacchetto di azzeramento con il proprio Source Address (SA), trasmette un nuovo token.

Se entro un tempo chiamato *Timer No Token* (TNT) l'active monitor non riceve il pacchetto di azzeramento con il proprio SA, entra in uno stato di standby monitor e allo scadere del tempo chiamato *Timer Standby Monitor* (TSM) inizia il processo di elezione dell'active monitor.

In presenza di un guasto anche il processo di token claim può fallire: in questo caso si attiva un processo di isolamento dei guasti (si veda il paragrafo 7.2.10).

7.2.9 Notifica della stazione vicina (neighbor notification)

L'active monitor invia periodicamente in broadcast, con periodo pari a TAM (*Timer Active Monitor*), dei pacchetti AMP che attivano anche il processo di notifica della stazione vicina. Tale processo permette ad ogni stazione di conoscere l'indirizzo della stazione collegata all'ingresso Ring-In, cioè la più vicina stazione "a monte" attiva, più vicina (NAUN: *Nearest Active Upstream Neighbor* o UNA: *Upstream Neighbor Address*).

La prima stazione attiva a valle dell'active monitor che riceve un pacchetto AMP esegue le seguenti operazioni:

- pone a 1 bit di address recognized e frame copied del pacchetto AMP;
- copia il pacchetto AMP ricevuto e memorizza l'indirizzo della stazione vicina da cui ha ricevuto il pacchetto in una locazione di memoria chiamata *Stored Upstream neighbor's Address* (SUA);
- trasmette in broadcast appena possibile un pacchetto chiamato SMP (*Standby Monitor Presence*) alla stazione successiva.

La stazione che riceve un pacchetto SMP memorizza a sua volta l'indirizzo della stazione vicina da cui ha ricevuto il pacchetto e trasmette un pacchetto SMP per poter notificare il proprio indirizzo alla stazione successiva.

Il processo di notifica continua fino a quando tutte le stazioni conoscono la propria stazione vicina, cioè il proprio UNA.

7.2.10 Isolamento dei guasti (beacon process)

Il processo di isolamento dei guasti viene attivato quando fallisce il processo di elezione dell'active monitor.

Una stazione D che abbia fallito il processo di claim token inizia il processo di isolamento dei guasti (figura 7.12) trasmettendo in broadcast un pacchetto di beacon che contiene l'indirizzo del proprio UNA (C) ed azzerando il *Timer Beacon Transmit* (TBT).

La stazione C verifica che il pacchetto di beacon ricevuto contenga come indirizzo del vicino (UNA) il proprio indirizzo MAC e poi entra in un stato di test escludendosi dal ring.

Se la verifica indica la stazione C come ben funzionante allora la stazione stessa si immette nuovamente del ring; in caso contrario la stazione rimane esclusa dal ring ed il guasto viene isolato.

Allo scadere del TBT la stazione D entra in uno stato di autoverifica escludendosi dal ring e verificando di non essere l'origine del guasto.

Entrambi i test comprendono anche la verifica delle connessioni con il concentratore.

Se sia C che D superano la fase di autotest, allora il guasto risiede nelle connessioni fisiche tra i concentratori o nei concentratori stessi.

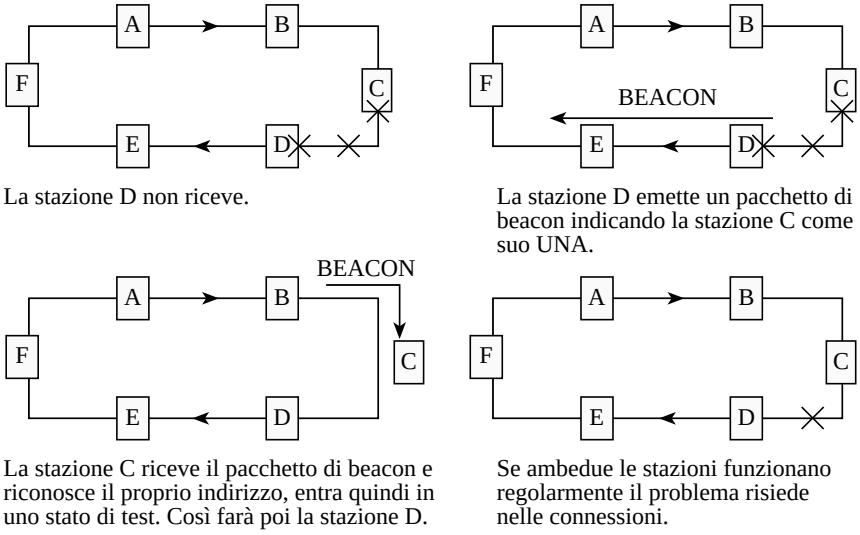

A
B
C
D
E
F
BEACON
La stazione D non riceve.
La stazione D emette un pacchetto di beacon indicando la stazione C come suo UNA.
La stazione C riceve il pacchetto di beacon e riconosce il proprio indirizzo, entra quindi in uno stato di test. Così farà poi la stazione D.
Se ambedue le stazioni funzionano regolarmente il problema risiede nelle connessioni.

Fig. 7.12 - Esempio di processo di beacon.

7.2.11 Rilascio anticipato del token (early token release)

Al crescere della velocità trasmissiva, il MAC a token sin qui descritto non aumenta le sue prestazioni in modo lineare. Per comprendere il perché analizziamo l'efficienza del Token Ring a 16 Mb/s per la trasmissione di un pacchetto da 256 ottetti.

Supponiamo, per esempio, di avere una rete di 260 stazioni aventi ognuna una lunghezza di lobo di 100 m: ne consegue che lo sviluppo totale dell'anello è di 260 x 200 m = 52 Km. La trasmissione di 256 ottetti impiega 256 x 8 x 62.5 ns = 128 μs. La velocità di propagazione di un cavo rame è di circa 200 m/μs, ne consegue che un pacchetto da 256 ottetti occupa circa 25.6 Km del ring, in quanto 128 x 200 = 25600 m. Quindi, nel caso preso in esame, avremo circa la metà dell'anello inutilizzata (bit di riempimento), con un'efficienza del MAC dimezzata.

Per superare tale limite è stata introdotta la possibilità, per il Token Ring a 16 Mb/s, di rilasciare il token alla fine della trasmissione del pacchetto, senza attendere che la stazione trasmittente riceva il campo di source address del pacchetto che ha trasmesso. Questa miglioria è detta *early token release*.

7.2.12 Priorità di accesso

La priorità di accesso consiste nella possibilità di trasmettere pacchetti a diverse priorità, a seconda dell'importanza della trasmissione, allo scopo di privilegiare applicazioni particolari, quali quelle real time.

La priorità di un token limita l'insieme delle stazioni che possono catturarlo a quelle con priorità maggiore o uguale a quella del token.

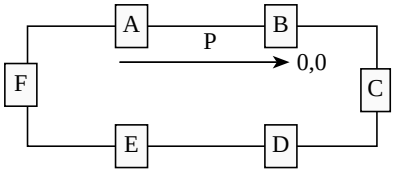
Una stazione che vuole trasmettere ad una data priorità deve richiedere che venga rilasciato un token a quella priorità, scrivendo la priorità richiesta nel sottocampo reservation bit del campo access control di un pacchetto in transito.

La stazione che genera il token può alzare la priorità, che normalmente è a zero, in base al valore dei bit di reservation del campo access control. Essa imposta i priority bit uguali ai reservation bit e poi azzera i reservation bit.

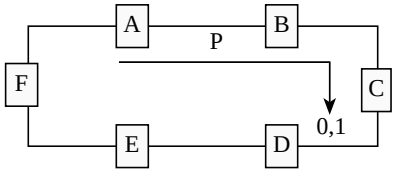
Durante il percorso di un pacchetto la priorità richiesta può crescere più volte: infatti una stazione può impostare una richiesta di priorità ad un certo valore e successivamente un'altra stazione può impostare una richiesta a priorità maggiore e quest'ultima rimpiazza quella precedente.

Soltanto la stazione che ha inzialmente elevato il valore di priorità d'accesso può successivamente riabbassarlo.

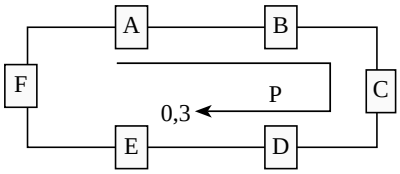
Le figure 7.13 e 7.14 mostrano le fasi di un processo di assegnazione della priorità.



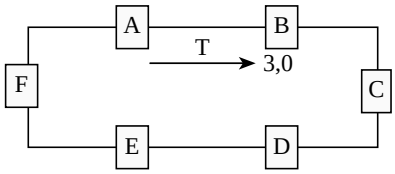
La stazione A sta trasmettendo un pacchetto per la stazione C, la stazione B vede passare il pacchetto P con priorità 0 e richiesta di priorità 0.



La stazione B imposta la richiesta di priorità a 1.

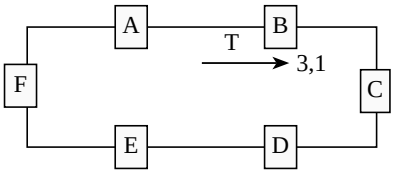


La stazione C copia il pacchetto. La stazione D imposta la richiesta di priorità a 3.

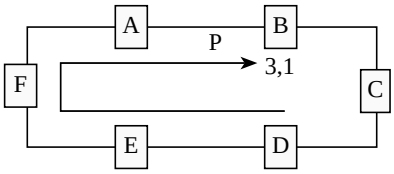


La stazione A rimuove il pacchetto ed emette un token con priorità 3.

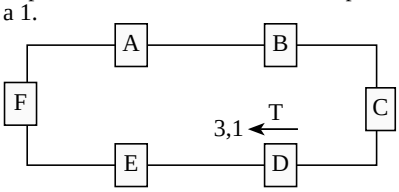
Fig. 7.13 - Esempio di assegnazione della priorità: prime 4 fasi.



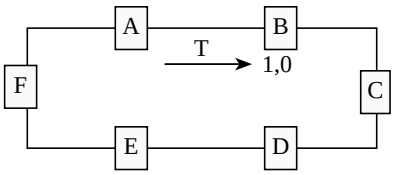
La stazione B (con priorità 1) vede il token con priorità 3, non può utilizzarlo, ma imposta nuovamente la richiesta di priorità a 1.



La stazione D cattura il token e trasmette un pacchetto con priorità 3.



La stazione D rimuove il pacchetto ed emette il token a priorità 3 e richiesta di priorità 1.



La stazione A riceve il token e cambia la priorità portandola a 1 ed ora la stazione B potrà trasmettere.

Fig. 7.14 - Esempio di assegnazione della priorità: ultime 4 fasi.

7.2.13 Inserzione della stazione sull'anello

Ogni stazione può richiedere al centro stella di essere inserita oppure no sull'anello. Tale richiesta viene effettuata con una differenza di potenziale continua che la stazione genera tra le coppie di Ring-In e Ring-Out. In assenza di differenza di potenziale (ad esempio, stazione spenta) la stazione è disinserita dall'anello (si veda il paragrafo 7.3.4).

7.2.14 Test della stazione

Prima dell'inserimento della stazione nel ring e durante il processo di isolamento dei guasti, la stazione si esclude dal ring e il concentratore richiude le coppie di Ring-In e di Ring-Out della stazione (stato di bypass in figura 7.2).

La stazione trasmette un pacchetto di *lobe media test* avente il destination address con valore zero; questo test serve per verificare il funzionamento globale del lobo che è costituito dalla stazione e dai cavi di collegamento al concentratore.

Se la stazione supera il lobe media test chiede al concentratore di essere inserita sull'anello.

7.2.15 Timer principali utilizzati da 802.5

Le principali funzioni del livello MAC sono governate da timer, allo scadere dei quali vengono intraprese le seguenti azioni:

- il *Timer Holding Token* (THT) indica il tempo massimo per cui una stazione può trattenere il token. Il valore massimo consentito è di 8.9 ms;
- il *Timer Valid Transmission* (TVX) indica il tempo massimo che può intercorrere tra due trasmissioni valide (di token o pacchetto). Il valore massimo consentito è di 10 ms;
- il *Timer No Token* (TNT) indica il tempo massimo di assenza del token, e viene usato per ricuperare varie situazioni di errore relative al token. Il valore massimo ammesso è di 2.6 s;
- il *Timer Active Monitor* (TAM) indica l'intervallo di tempo che intercorre tra due richieste di notifica delle stazioni vicine provocate dall'active monitor. Il valore massimo consentito è di 7 s;
- il *Timer Standby Monitor* (TSM) è utilizzato dalle stazioni che sono in stato di standby monitor per rilevare la presenza dell'active monitor e dei token. Il valore massimo consentito è di 15 s;

- il *Timer Beacon Transmit* (TBT) indica il tempo in cui una stazione può rimanere nello stato di trasmissione di beacon prima di andare in una condizione di bypass. Il valore massimo consentito è di 160 ms.

7.3 IL LIVELLO FISICO

Il livello fisico di Token Ring varia in funzione dello standard considerato.

La versione ISO 8802.5 definisce l'utilizzo del cavo STP a 150 Ω (si veda il paragrafo 3.2.10) e di concentratori passivi chiamati MAU (*Multistation Access Unit*).

La bozza 802.5 Q/Draft 3 permette l'utilizzo di cavi UTP di categoria 3, 4, 5 (si veda il paragrafo 3.2.13) per la velocità di 4 Mb/s e di categoria 4 e 5 per la velocità di 16 Mb/s; introduce inoltre nuove famiglie di concentratori attivi e parzialmente attivi.

7.3.1 Il Jitter

Uno dei problemi più complessi a livello fisico che i costruttori di componenti elettronici hanno dovuto risolvere, è stato quello di compensare il *jitter*, cioè la variazione temporale spuria della fase del segnale causata principalmente dai componenti passivi quali i cavi, i connettori ed i concentratori passivi.

In una rete Token Ring è l'active monitor che genera il clock, tutte le altre stazioni si sincronizzano sul clock dell'active monitor durante la ricezione del token, dei pacchetti o dei bit di riempimento. Questi ultimi devono essere almeno 20 e precedono sempre qualunque tipo di trasmissione. La sincronizzazione viene effettuata da appositi circuiti della stazione ricevente che agganciano in fase il loro clock con quello della precedente stazione trasmittente.

Un jitter troppo elevato può comportare una non corretta sincronizzazione di una o più stazioni rispetto al clock dell'active monitor. Per questa ragione lo standard ha imposto regole di configurazione molto restrittive riguardanti il numero massimo di stazioni e di concentratori in un anello e la lunghezza massima dei lobi.

Per compensare i problemi di sfasamento dovuti al fenomeno del jitter è stato aggiunto un *elasticity buffer* (si veda figura 7.5) che può essere espanso a seconda della necessità, per mantenere costante la latenza totale.

7.3.2 Il cablaggio

Il percorso delle informazioni in una rete Token Ring è ad anello, ma il cablaggio tra le stazioni ed il concentratore è a stella. La connessione tra il concentratore e la stazione si

chiama *lobo* ed include i cavi di cablaggio, i cavetti di permutazione ed i connettori. I concentratori sono collegati a doppio anello controrotante tramite un anello primario e uno di backup (si veda il paragrafo 3.5.2). La figura 7.15 mostra un esempio di rete Token Ring.

La connessione fisica della stazione al mezzo trasmissivo viene effettuata tramite un cavo STP che presenta dal lato stazione un connettore di tipo DB9 e dal lato concentratore un connettore ermafrodita (si veda il paragrafo 4.2.1).

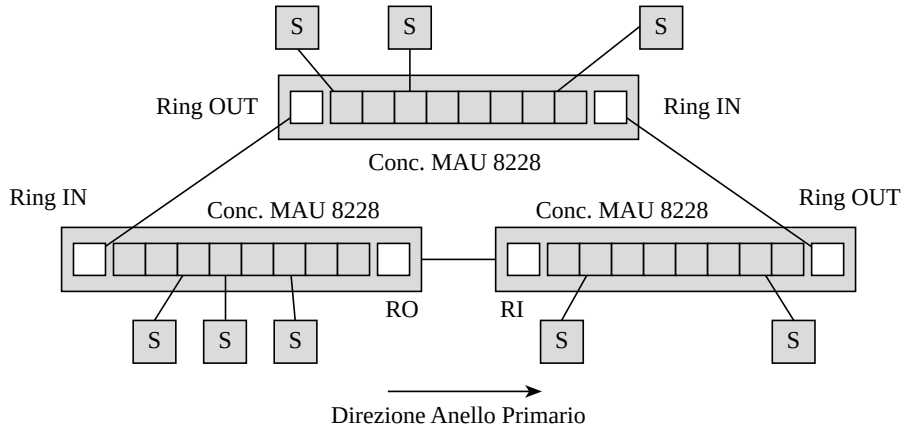


Fig. 7.15 - Esempio di una rete Token Ring.

Qualora il cablaggio venga realizzato con cavo UTP bisogna inserire un *media filter* tra la stazione ed il cavo, con lo scopo di adattare l'impedenza da 150 a 100 Ω e di ridurre l'emissione di disturbi elettromagnetici. Il media filter presenta due diversi tipi di connettori: un DB9 che va connesso alla stazione ed un RJ45 (si veda il paragrafo 4.4.5) a cui va connesso il cavo UTP.

Quando si usano i cavi UTP bisogna installare i media filter sulle stazioni, mentre dal lato concentratore non è necessario in quanto le porte o sono passive, o sono attive e hanno già l'impedenza corretta.

7.3.3 Interfacciamento al mezzo trasmissivo

Lo standard usa le seguenti abbreviazioni per indicare i componenti passivi utilizzati nell'interconnessione tra stazione e concentratore:

- *MIC (Medium Interface Connector).* Si riferisce al connettore presente sulla stazione, sul concentratore e sui cavi;

- *CMIC*. MIC presente sul concentratore;
- *MIC_S*. Si riferisce al connettore per il cavo STP (connettore ermafrodita);
- *MIC_U*. Si riferisce al connettore per il cavo UTP (connettore RJ45);
- *Lobe cable.* È il cavo di connessione tra la stazione ed il concentratore;
- *Trunk cable.* È il cavo di interconnessione tra i concentratori;
- *TCU (Trunk Coupling Unit).* È la porta di lobo del concentratore.

I concentratori vengono forniti con connettori di tipo ermafrodita nel caso di cablaggio STP, o con connettori di tipo RJ45 nel caso di cablaggio UTP.

La figura 7.16 mostra un esempio di connessione tra la stazione ed il mezzo trasmissivo.

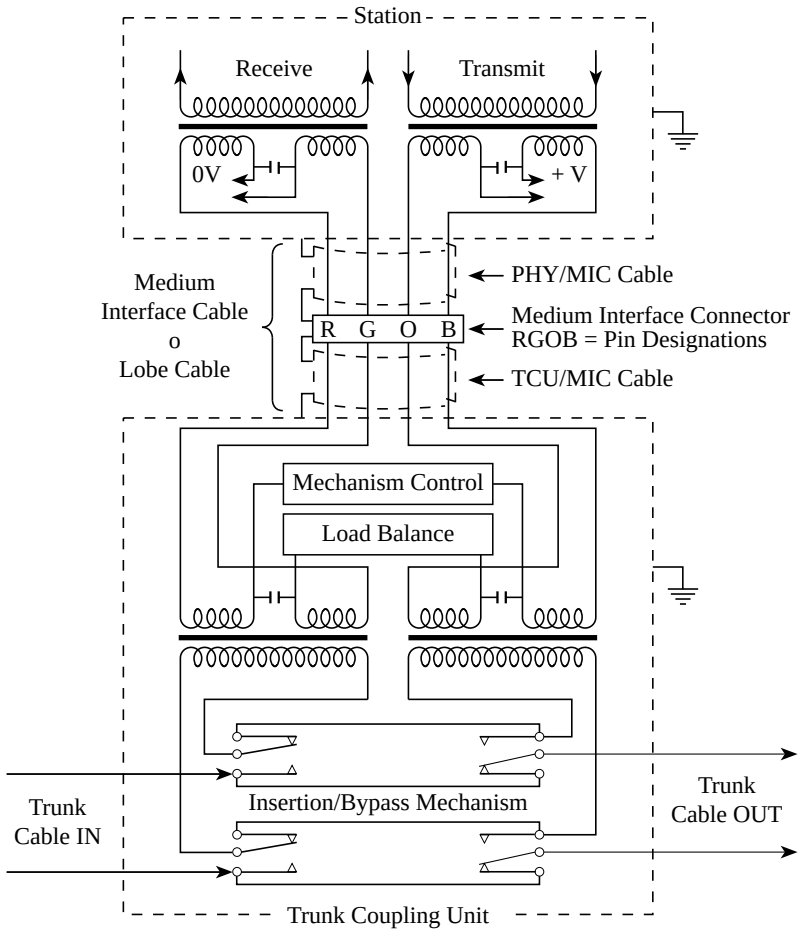


Fig. 7.16 - Esempio di interconnessione.

7.3.4 Controllo di accesso al ring fisico

Quando una stazione è attiva può richiedere al concentratore di essere inserita nell'anello. A tal fine genera una differenza di potenziale continua tra la coppia di Ring-In e la coppia di Ring-Out, compresa tra 3.5 e 7 V, detta tensione d'inserzione. Tale differenza di potenziale permette al relé di commutare dalla condizione di riposo (stazione esclusa), alla condizione di lavoro (stazione inserita).

La stazione ha un circuito di controllo di accesso all'anello che fornisce o rimuove la tensione d'inserzione a seconda che la stazione debba essere inserita nell'anello o debba essere in bypass per scopi di test o a causa di guasti (si veda la figura 7.5).

7.3.5 Ripetizione dei pacchetti ricevuti

La ripetizione dei pacchetti ricevuti è demandata al circuito di repeat path (si veda figura 7.5) il quale è controllato dal livello MAC che determina l'abilitazione o disabilitazione della funzione di ripetizione.

7.3.6 Codifica e decodifica dei segnali

Le stazioni Token Ring codificano e decodificano le trasmissioni secondo il metodo Manchester (si veda il paragrafo 3.1.2) che consente anche di ricavare il clock dai pacchetti ricevuti. Solo l'active monitor genera il clock con il proprio oscillatore interno.

Per assicurare una corretta circolazione del token nell'anello è necessario che il ring abbia un tempo di latenza minimo pari alla lunghezza del token. Per questa ragione le stazioni sono provviste di un circuito detto *latency buffer* che può introdurre ritardo pari a 24 bit time. La latenza di 24 bit time viene fornita dalla stazione che è l'active monitor.

7.3.7 I concentratori

I concentratori servono per connettere le stazioni all'anello tramite un cablaggio stellare, possono avere un numero di porte di lobo compreso tra 8 e 20 e sono in grado di operare a 4 e 16 Mb/s.

Ci possono essere tre tipi di concentratori :

- *Passivi*. Sono composti dai connettori e dai relay di bypass/inserzione sulle porte di lobo. Non hanno meccanismi automatici di bypass dei guasti sulle porte di dorsale. Esempio: IBM 8228.

- *Attivi*. Sono equipaggiati con circuiti di amplificazione e retiming su ogni porta e vengono utilizzati normalmente con i cavi UTP. Hanno meccanismi automatici di bypass dei guasti sulle porte di dorsale. Esempio: IBM 8230, modello 2 attivo.
- *Parzialmente attivi*. Hanno circuiti di amplificazione e retiming solo sulle porte di dorsale, mentre quelle di lobo sono passive. Hanno meccanismi automatici di bypass dei guasti sulle porte di dorsale. Esempio: IBM 8230 modello passivo.

I concentratori passivi (figura 7.17) sono i primi nati, ma sono ormai stati sostituiti dagli altri due tipi, in quanto, alla velocità di 16 Mb/s, imponevano comunque l'aggiunta di ripetitori .

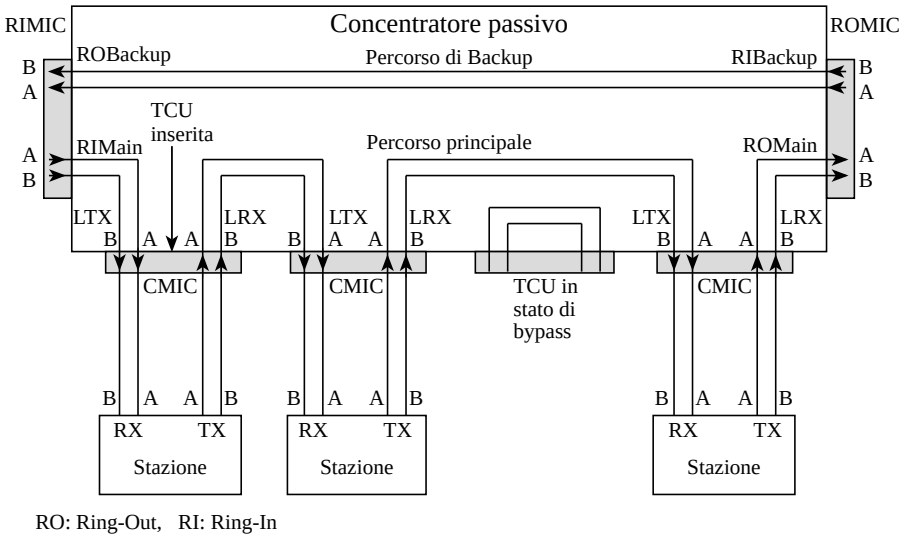


Fig. 7.17 - Concentratore passivo.

Nei concentratori passivi il percorso di backup può essere utilizzato solo se le porte di dorsale sono connesse a ripetitori. In tal caso è il ripetitore che ha la capacità in caso di guasto di richiudere automaticamente l'anello primario sul percorso di backup. In alternativa si può disconnettere manualmente il cavo da una porta di dorsale e il connettore stesso è costruito in modo da richiudere l'anello primario sul percorso di backup.

I concentratori attivi sono stati sviluppati per utilizzare i cavi UTP senza imporre grosse limitazioni di configurazione. Essi rappresentano la miglior soluzione per i sistemi di cablaggio in quanto offrono una grande flessibilità e semplificano molto le regole di configurazione. Essi vengono anche chiamati *Active Retimed Concentrator*

(ARC) in quanto tutte le porte sono equipaggiate con un ripetitore e quindi eseguono funzioni di amplificazione e retiming del segnale. Le porte dei concentratori attivi contengono anche il media filter (figura 7.18).

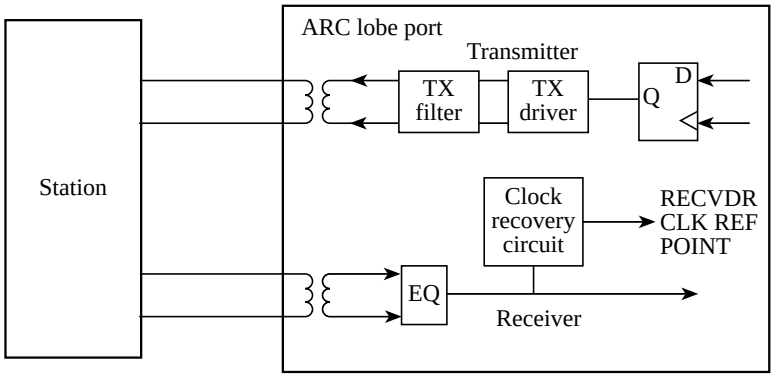


Fig. 7.18 - Porta di lobo attiva.

I concentratori parzialmente attivi rappresentano una buona soluzione per i sistemi di cablaggio basati su cavi STP o UTP ed impongono regole meno restrittive rispetto a quelli totalmente passivi.

La figura 7.19 mostra un esempio di concentratore parzialmente attivo.

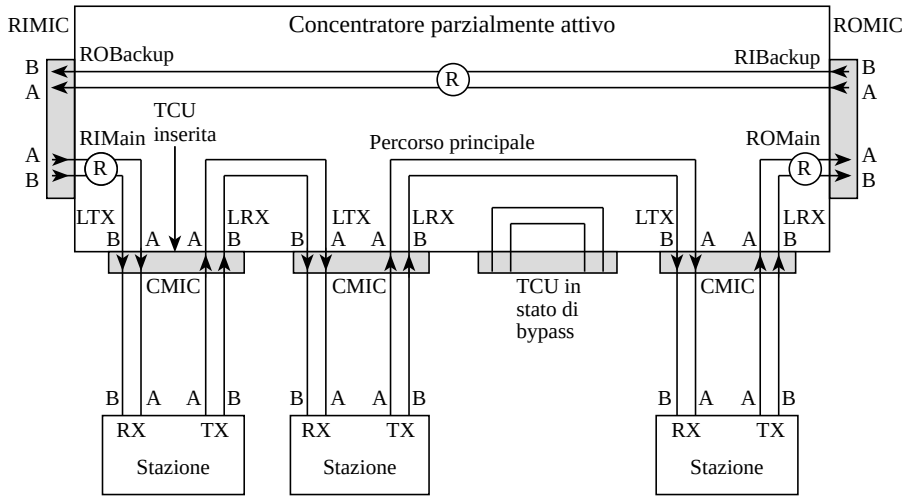


Fig. 7.19 - Concentratore parzialmente attivo.

Le connessioni tra concentratore e stazione sono riportate nella figura 7.20 e sono indipendenti dal tipo di concentratore.

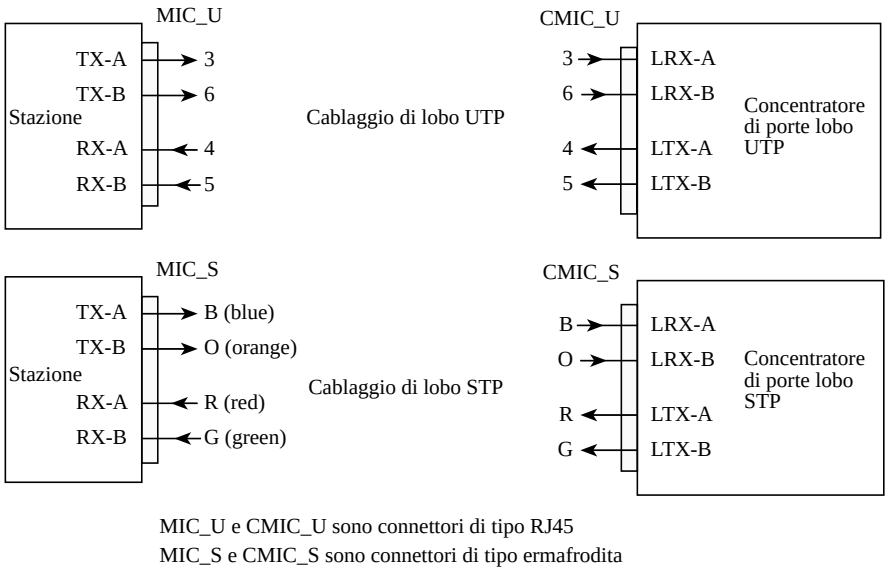


Fig. 7.20 - Connessioni fra stazione e concentratore.

Per interconnettere due concentratori distanti fra loro si possono utilizzare ripetitori in fibra ottica che permettono connessioni fino a 2 Km di distanza. Alcuni costruttori offrono dei ripetitori in fibra ottica con doppia connessione: una principale ed una ridondante, per ragioni di tolleranza ai guasti.

7.4 REGOLE DI CONFIGURAZIONE

Le prime regole di configurazione sono state sviluppate da IBM ed erano basate sull'utilizzo di una serie di tabelle che, a seconda delle velocità trasmissive, del numero di concentratori e delle distanze tra questi, fornivano la lunghezza massima di lobo.

Queste regole si sono rivelate imprecise, in quanto non consideravano una serie di parametri quali:

- l'attenuazione del concentratore causata dalla perdita di segnale sui contatti del relé e sui connettori;
- il valore di diafonia combinata (combined NEXT), che dipende dal numero di concentratori e componenti passivi che sono connessi fra loro in modalità seriale.

Il parametro principale per il corretto funzionamento della rete è il rapporto tra il segnale attenuato e il segnale indotto dalla coppia vicina (si veda il paragrafo 3.2.5). Questo parametro viene indicato col nome ACR (*Attenuation to Cross-talk Ratio*) dal comitato ISO/IEC e definito col nome NIR (*Next loss to Insertion loss Ratio*) dalla bozza 802.5 Q/D3.

Il comitato americano IEEE ha sviluppato in modo approfondito le problematiche associate al NIR ed ha imposto regole molto restrittive riguardanti il numero massimo di concentratori e di stazioni, e le distanze massime percorribili.

Una progettazione di rete deve considerare sempre le regole più restrittive per garantire un buon funzionamento in tutte le condizioni possibili. Per questa ragione è consigliabile progettare la rete in modo che possa funzionare correttamente sia a 4 sia a 16 Mb/s.

7.5 REGOLE IBM

Le regole da rispettare riguardano il massimo numero di stazioni e la distanza massima di lobo.

Il numero massimo di stazioni consentito è 260 e questa limitazione dipende dal livello MAC. Ogni ripetitore per cavo in rame riduce di una stazione il numero massimo consentito ed ogni convertitore in fibra ottica comporta una riduzione di due stazioni.

Nella terminologia IBM un MAU è contenuto all'interno di un armadio e più armadi adiacenti formano una *cabina*.

La distanza massima di lobo si calcola in modo diverso se la rete è realizzata con una cabina singola o con più cabine distanti fra loro.

Il caso peggiore si ha quando il doppio anello controrotante di dorsale si ripiega sul percorso di backup, per un guasto. Se il guasto è sul cavo di dorsale di lunghezza minore, allora l'anello assume la lunghezza maggiore.

Per questa ragione, in fase di progetto, è opportuno calcolare la lunghezza adattata dell'anello, chiamata ARL *(Adjusted Ring Length),* che si ricava sottraendo alla lunghezza totale del ring la distanza più breve tra due cabine.

Supponiamo ad esempio di avere 3 MAU concentrator su piani diversi di un edificio. Essi vanno considerati come tre cabine contenenti ciascuna un MAU. Se le tre distanze sono 10, 5, 15 m, la lunghezza adattata dell'anello è uguale a 10+5+15-5, cioè 25 m.

Le formule riportate nel seguito evitano l'uso delle tabelle IBM ed offrono un risultato mediato un po' più restrittivo e quindi più sicuro. Si assume di utilizzare cavo di tipo 1 e MAU 8228.

NA indica il numero di armadi, NM indica in numero di MAU e NC indica il numero di cabine.

7.5.1 Cablaggio con cabina singola

A 4 Mb/s lunghezza di lobo = 390 - NA · 5 - NM · 5
A 16 Mb/s lunghezza di lobo = 178 - NA · 5 - NM · 5

7.5.2 Cablaggio con più cabine

A 4 Mb/s lunghezza di lobo = 395 - NC · 5 - NM · 9 - ARL
A 16 Mb/s lunghezza di lobo = 189 - NC · 5 - NM · 9 - ARL

Si osservi che per un Token Ring a 16Mb/s con 50 stazioni, 8 MAU, 3 cabine e ARL di 25 m, la lunghezza di lobo è di 77 m, inferiore a quella prevista dagli standard sul cablaggio strutturato. Per poter realizzare una rete di questo tipo bisogna ricorrere a ripetitori o a concentratori attivi o parzialmente attivi.

7.6 REGOLE 802.5

Lo standard 802.5 stabilisce i valori massimi di attenuazione e diafonia accettati per connettori, concentratori e cavi.

Per quanto riguarda i cavi fa riferimento allo standard EIA/TIA 568 ed ai successivi bollettini TSB 36 e 40.

Per i connettori richiede le seguenti caratteristiche minime:

- connettore per STP (ermafrodita): -62 dB minimo di diafonia nelle frequenze comprese tra 100 KHz e 4 MHz, -50 dB minimo di diafonia nelle frequenze comprese tra 4 e 16 MHz, 0.1 dB massimo di perdita d'inserzione nelle frequenze comprese tra 100 KHz e 16 MHz;
- connettore per UTP (RJ45): -56 dB minimo di diafonia nelle frequenze tra 0.1 e 16 MHz, 0.1 dB massimo di perdita d'inserzione nelle frequenze comprese tra 1 e 16 MHz.

Per i concentratori passivi l'attenuazione massima consentita è di 2 dB ed il valore minimo di diafonia deve essere -40 dB nelle frequenze comprese tra 4 e 24 MHz.

L'attenuazione riferita ai concentratori passivi viene anche detta 'flat attenuation', in quanto non è in funzione della frequenza, ma dipende principalmente dalla perdita d'inserzione dei contatti dei relé.

7.6.1 Attenuazione massima

La perdita massima ammessa nel percorso tra due elementi attivi, siano essi due stazioni, nel caso di utilizzo di concentratori passivi, o una stazione e una porta di un concentatore attivo, è la seguente:

- 19 dB a 4 e 16 Mb/s quando si utilizzano concentratori passivi;
- 19 dB a 4 Mb/s quando si utilizzano concentratori attivi;
- 16 dB a 4/16 e 16 Mb/s quando si utilizzano concentratori attivi.

Quando si parla di velocità 4/16 Mb/s ci si riferisce a stazioni che usano componenti elettronici che possono funzionare a 4 e 16 Mb/s.

7.6.2 Rapporto segnale/disturbo

I valori minimi richiesti di NIR in un percorso tra due elementi attivi sono i seguenti:

- 19 dB con l'utilizzo di cavi STP e concentratori attivi o passivi, a 4 Mb/s;
- 17.5 dB con l'utilizzo di cavi UTP e concentratori attivi o passivi, a 4 Mb/s;
- 17 dB con l'utilizzo di cavi STP e concentratori passivi, a 4/16 e 16 Mb/s;
- 15.5 dB con l'utilizzo di cavi STP e concentratori attivi, a 4/16 e 16 Mb/s;
- 15.5 dB con l'utilizzo di cavi UTP e concentratori passivi, a 4/16 e 16 Mb/s;
- 14 dB con l'utilizzo di cavi UTP e concentratori attivi, a 4/16 e 16 Mb/s.

7.6.3 Numero massimo di stazioni

La limitazione del numero di stazioni dipende da due fattori: il livello MAC, che limita ad un massimo di 260 stazioni, ed il jitter accumulato.

Quando si usano i concentratori passivi il numero massimo di elementi di ripetizione è 300, di cui:

- 260 possono essere stazioni;
- 40 possono essere altri elementi di ripetizione.

Quando si usano i concentratori attivi il numero massimo di elementi di ripetizione è 300, di cui:

- 144 possono essere stazioni;
- 144 possono essere le porte attive dei concentratori;

- 12 possono essere altri elementi di ripetizione.

Si noti che i concentratori attivi riducono il numero massimo di stazioni collegabili da 260 a 144, aumentando però, come vedremo nel seguito, la lunghezza massima del lobo. D'altro canto, gli esempi seguenti dimostrano come, utilizzando esclusivamente concentratori passivi e volendo mantenere la lunghezza di lobo pari a 100 m, non si riesca ad andare oltre le 40 stazioni.

7.6.4 Utilizzo di soli concentratori passivi

Utilizzando concentratori passivi la distanza di lobo massima è molto complessa da calcolare, poiché si sommano i valori di attenuazione dei vari elementi, ma soprattutto si combinano i valori di diafonia dei vari componenti.

Si considerino, ad esempio, i tre seguenti tipi di concentratori:

- a 8 porte avente un'attenuazione di 0.5 dB ed una diafonia di -40 dB;
- a 12 porte avente un'attenuazione di 0.8 dB ed una diafonia di -40 dB;
- a 20 porte avente un'attenuazione di 1.3 dB ed una diafonia di -40 dB.

Analizziamo il numero massimo di concentratori utilizzabili in una rete a cabina singola, a 16 Mb/s, per ottenere una lunghezza di lobo di 100 m.

Con il cavo STP a 150 Ω il numero massimo di concentratori è il seguente:

- 5 concentratori a 8 porte, oppure
- 4 concentratori a 12 porte, oppure
- 3 concentratori a 20 porte.

Con il cavo UTP di categoria 5 il numero massimo di concentratori è il seguente:

- 4 concentratori a 8 porte, oppure
- 3 concentratori a 12 porte, oppure
- 2 concentratori a 20 porte.

7.6.5 Cavi utilizzabili

Se si usano concentratori passivi o parzialmente attivi bisogna usare cavi STP o UTP di categoria 5.

Se si usano concentratori attivi si possono usare cavi STP o UTP di categoria 4 e 5.

7.6.6 Concentratori attivi o parzialmente attivi

Entrambi i tipi forniscono lunghezze di lobo maggiori o uguali ai 100 m previsti dagli standard di cablaggio strutturato e specificate dal costruttore del concentratore, in funzione del tipo di cavo. Ed esempio, il MAU IBM 8230, parzialmente attivo, quando usato con cavo STP di tipo 1 IBM, fornisce una lunghezza di lobo di 145 m.

Nel caso di concentratori attivi si ottengono le seguenti lunghezze di lobo:

- cavo STP 340 m;
- cavo UTP cat. 5 195 m;
- cavo UTP cat. 4 150 m.

BIBLIOGRAFIA

[1] IBM Centro di competenza Telecomunicazioni, "Reti Locali IBM: Sistema di cablaggio IBM", Codice documento GA13-1536-01, Roma (Italia), settembre 1989.

[2] IBM, "Token-Ring Network: Architecture Reference", Pub. No. SC30-3374-01, second edition, August 1987.

[3] ISO/IIEC 8802.5, IEEE Std 802.5, "Token ring access method and physical layer specifications", First Edition, June 1992.

[4] P 802.5 Q/D3 Standard project, Token Ring STP/UTP revision, March 1993.

[5] EIA/TIA-568, Commercial Building Telecommunications Wiring Standard (ANSI/EIA/TIA-568-91), July 1991.

[6] TSB-36, Additional Cable Specifications for Unshielded Twisted Pair Cables, November 1991 (used in conjunction with EIA/TIA wiring standard.)

[7] TSB-40, Additional Transmission Specification for Unshielded Twisted-Pair Connecting hardware, August 1992 (used in conjunction with EIA/TIA wiring standard and TSB36 above).

8

LA RETE FDDI E LO STANDARD ISO 9314

8.1 INTRODUZIONE

Nel 1982 il sottocomitato X3T9.5 dell'ANSI (*American National Standard Institute*) inizia lo sviluppo di una rete locale ad alta velocità (100 Mb/s) detta FDDI (*Fiber Distributed Data Interface*, figura 8.1). FDDI nasce per operare sulla fibra ottica e successivamente introduce anche l'uso di doppini in rame per le connessioni tra le stazioni ed i concentratori.

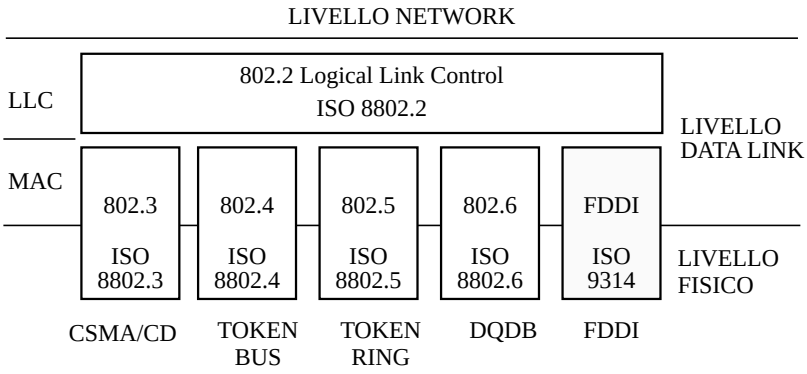


Fig. 8.1 - Relazioni tra i livelli OSI e FDDI.

Lo standard FDDI è costituito da 4 elementi (figura 8.2) a cui si riferiscono i relativi sotto-standard. Essi sono: il PMD *(Physical Medium Dependent), il* PHY *(livello fisico), il* MAC *(Media Access Control), lo* SMT *(Station Management).*

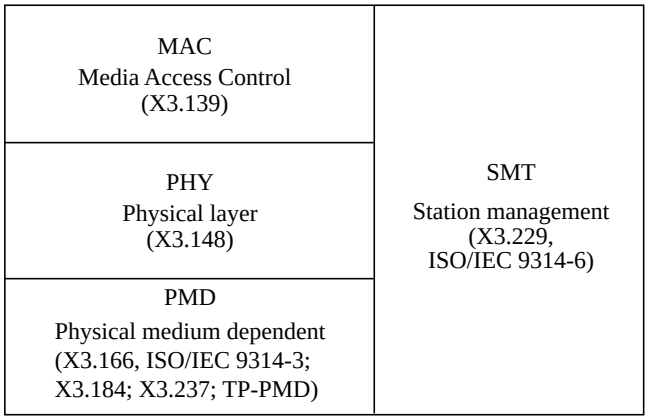


Fig. 8.2 - Elementi componenti lo standard FDDI.

8.1.1 Gli standard di FDDI

Alla fine del 1986 il comitato ANSI approva lo standard X3.139, che tratta le specifiche FDDI del livello MAC, nella prima metà del 1988 approva lo standard X3.148, che tratta le specifiche del livello PHY, nella seconda metà del 1989 approva lo standard X3.166 che tratta le specifiche della parte PMD riguardante l'utilizzo della fibra ottica multimodale. Quest'ultimo viene adottato nel 1990 come standard internazionale ISO/IEC 9314-3.

La definizione del livello di gestione SMT ha richiesto più tempo degli altri livelli e quindi i costruttori di apparati FDDI hanno adottato le specifiche contenute nelle bozze di progetto disponibili al momento dello sviluppo del prodotto. Solamente alla fine del 1993 il comitato ANSI pubblica la bozza di standard X3.229 che include le precedenti bozze X3T9.5/84-49 e X3T9.5/92-67 e viene adottata anche dal comitato internazionale prendendo il nome di bozza ISO/IEC 9314-6. I prodotti FDDI installati possono quindi avere revisioni diverse del firmware relativo alla parte SMT e, per garantire una completa compatibilità, è preferibile che tutti i prodotti siano aggiornati all'ultima versione.

La necessità di aver a disposizione distanze maggiori tra le stazioni FDDI ha determinato lo sviluppo di un ulteriore standard che definisce le specifiche per l'utilizzo della fibra monomodale. Esso prende il nome di X3.184-1993 ed è stato approvato all'inizio del 1993.

Gli apparati FDDI non hanno avuto, negli anni passati, il successo sperato per due ragioni principali: la prima è che non si è verificata una grande necessità di banda

trasmissiva, la seconda è che i costi degli apparati erano troppo elevati. Per quest'ultima ragione sono stati sviluppati altri due standard che riducono i costi dei componenti e dell'installazione. Alla fine del 1992 il comitato ANSI pubblica la bozza di standard X3.237 che include le specifiche delle precedenti bozze X3T9.5/92 e LCF-PMD/079, e fornisce le specifiche per l'utilizzo di componenti per fibre ottiche multimodali a basso costo. All'inizio del 1994 viene pubblicata la bozza di standard TP-PMD che include le specifiche delle precedenti bozze X3T9/93-130, X3T9.5/93-022 e TP-PMD/306, e fornisce le specifiche per l'utilizzo di cavi STP e UTP.

8.1.2 Le stazioni FDDI

Le stazioni di una rete FDDI possono essere dei seguenti tipi:

- schede di interfaccia per calcolatori (mainframe, minicomputer, workstation, PC);
- Bridge FDDI/(Ethernet e IEEE 802.3), FDDI/802.5, FDDI/FDDI;
- Router/Brouter;
- Gateway;
- *Dual Attachment Concentrator* (DAC).

8.1.3 PMD

Il PMD è lo strato più basso del livello Fisico della pila OSI e descrive le specifiche hardware per la connessione delle stazioni FDDI ed in particolare le interfacce verso i mezzi trasmissivi, i livelli dei segnali, le caratteristiche dei circuiti ricevitori e trasmettitori, le caratteristiche dei connettori e dei mezzi trasmissivi.

8.1.4 PHY

Il PHY è lo strato più alto del livello Fisico e si occupa principalmente della codifica e decodifica dei pacchetti, della sincronizzazione, della combinazione e separazione di clock e dati, della compensazione di differenze di clock tra stazioni adiacenti.

8.1.5 MAC

Il MAC è lo strato più basso del livello Data Link e fornisce i servizi di accesso all'anello, inizializzazione dell'anello e isolamento dei guasti.

8.1.6 SMT

Lo SMT fornisce i servizi di monitoraggio e controllo di una stazione FDDI, ed in particolare si occupa dell'inserzione e rimozione di una stazione dall'anello, dell'inizializzazione di una stazione, della gestione della configurazione della stazione, dell'isolamento dei guasti, del recupero della funzionalità globale della rete e della raccolta di statistiche.

8.2 METODO DI ACCESSO TIMED TOKEN PASSING

Il MAC di FDDI viene comunemente chiamato *timed token passing* in quanto indica un sistema a token controllato da timer. I dati vengono trasmessi serialmente come stringhe di simboli da una stazione ad un'altra ed ogni stazione ripete le stringhe di simboli ricevute a quella successiva.

Il *simbolo* è l'elemento di rappresentazione più piccolo usato dal MAC e consiste in un quartetto (4 bit) che viene codificato/decodificato in un gruppo di 5 bit dal livello fisico in fase di trasmissione/ricezione (codifica 4B/5B, paragrafo 3.1.3). Si possono avere simboli di dato o di controllo.

Una rete FDDI ha le seguenti caratteristiche:

- la velocità di trasmissione è di 100 Mb/s al livello Data Link e 125 Mb/s sul mezzo trasmissivo a causa della codifica 4B/5B;
- la topologia è ad anello, ma può essere riportata a stella tramite l'uso di concentratori attivi.

L'anello FDDI offre inoltre caratteristiche di tolleranza ai guasti e di elevata affidabilità, ragioni per le quali si presta ad essere utilizzato come dorsale interconnettente altre sottoreti quali Ethernet e Token Ring.

La topologia logica è costituita da un anello monodirezionale, quella fisica è costituita da un *doppio anello controrotante*, avente un anello primario (*primary ring*) utilizzato per trasmettere i dati ed un anello secondario (*secondary ring*) che serve come percorso di backup (si veda il paragrafo 3.5.2). In condizioni normali (figura 8.3) le informazioni viaggiano sull'anello primario, mentre quello secondario si trova in uno stato di stand-by caldo (IDLE).

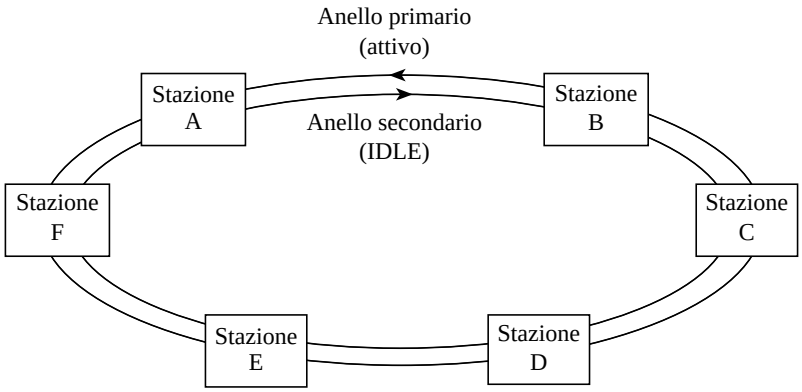


Fig. 8.3 - Anello FDDI.

In condizioni di guasto l'anello primario si richiude sul percorso di backup (figura 8.4) che abbandona lo stato di idle e fa fluire le informazioni: queste viaggiano lungo un percorso costituito dalla porzione di anello primario funzionante più quella dell'anello secondario (si veda anche il paragrafo 3.5.2).

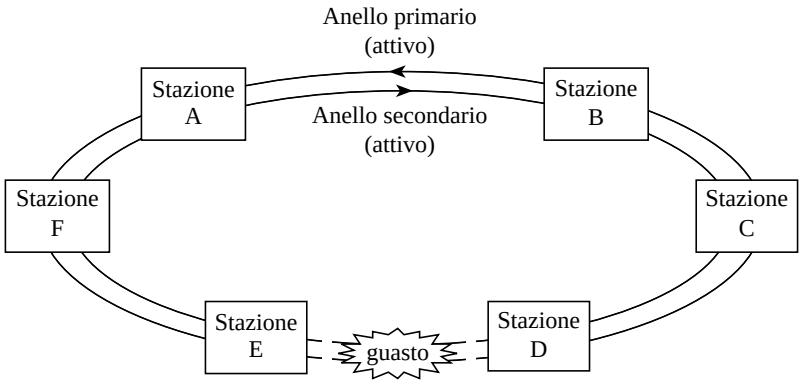


Fig. 8.4 - Caso di guasto dell'anello FDDI.

8.2.1 Trasmissione dei pacchetti

La trasmissione può essere di due tipi:

- sincrona, quando esiste l'esigenza di un tempo di risposta o di una banda garantiti (trasmissione voce e video);

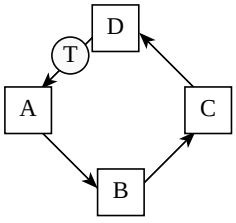
- asincrona, quando la banda viene allocata in modo dinamico; questa modalità è quella più comune in quanto è utilizzata per la trasmissione dati.

La modalità sincrona è prioritaria rispetto alla asincrona. Quando una stazione cattura il token trasmette sempre prima eventuali trame sincrone e poi, se rimane tempo, altre trame asincrone.

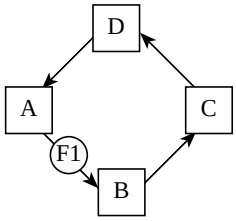
La modalità asincrona è molto simile al MAC di IEEE 802.5 con early token release: una stazione che ha dei pacchetti da trasmettere attende di ricevere il *token*, e quando lo cattura inizia la trasmissione dei pacchetti che deve completarsi entro un tempo limite definito dal timer THT (*Token Holding Timer*). In IEEE 802.5 il valore di THT è fisso, mentre in FDDI THT viene inizializzato dinamicamente ad un opportuno valore (si veda il paragrafo 8.2.10) in modo da garantire un tempo di rotazione massimo del token e quindi assicurare la banda necessaria alla trasmissione sincrona. Se il valore di THT risulta essere zero la stazione deve attendere il prossimo passaggio del token per poter trasmettere. Alla fine della trasmissione la stazione emette un nuovo token in modo da offrire la possibilità di trasmettere ad altre stazioni. Quando la stazione trasmittente riceve il pacchetto da essa generato lo rimuove dal ring. Durante la fase di trasmissione la funzione di ripetizione viene inibita.

La figura 8.5 e la figura 8.6 mostrano un esempio di trasmissione e ricezione di pacchetti lungo un'ipotetica rete FDDI.

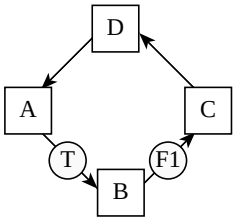
- Nella fase 1 la stazione A ha un pacchetto da trasmettere alla stazione C, attende il token e lo cattura.
- Nella fase 2 la stazione A inizia a trasmettere il pacchetto F1.
- Nella fase 3 la stazione A, alla fine della trasmissione del pacchetto, riemette il token; nel frattempo il pacchetto F1 si è propagato lungo l'anello ed ha raggiunto la stazione C la quale, osservando il campo destination, riconosce che il pacchetto è destinato ad essa e quindi inizia la copia del medesimo; alla fine della copia la stazione C imposta il bit di copied nel campo di frame status di F1.
- Nella fase 4 la stazione B, che aveva da trasmettere il pacchetto F2 alla stazione D, cattura il token ed inizia a trasmettere.
- Nella fase 5 la stazione B, alla fine della trasmissione del pacchetto, riemette il token; nel frattempo i pacchetti si sono ulteriormente propagati lungo l'anello e quello F2 raggiunge la stazione D la quale, osservando il campo destination, riconosce che il pacchetto è destinato ad essa e quindi inizia la copia del medesimo; alla fine della copia la stazione D imposta il bit di copied nel campo di frame status di F2.



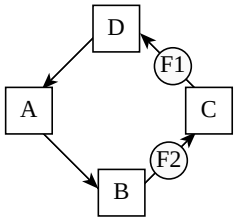
1 - A deve trasmettere e quindi cattura il token



2 - A inizia a trasmettere

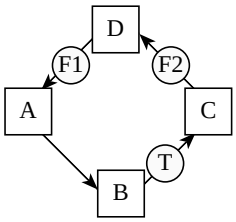


3 - Dopo i dati A ritrasmette il token

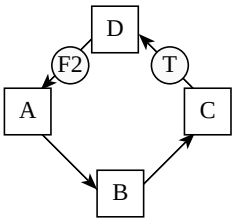


4 - B cattura il token e inizia a trasmettere

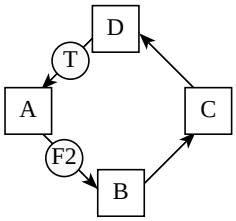
Fig. 8.5 - Esempio di trasmissione dati (fasi 1, 2, 3, 4).



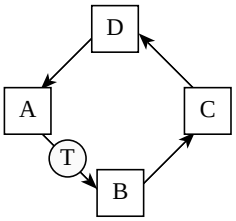
5 - B emette il token



6 - A toglie F1



7 - A ritrasmette F2 e il token



8 - B toglie F2

Fig. 8.6 - Esempio di trasmissione dati (fasi 5, 6, 7, 8).

- Nella fase 6 la stazione A riceve il pacchetto da essa trasmesso, lo riconosce confrontando il campo di source address con il proprio indirizzo e quindi lo rimuove dall'anello.
- Nella fase 8 la stazione B riceve il pacchetto da essa trasmesso e quindi lo rimuove dall'anello.

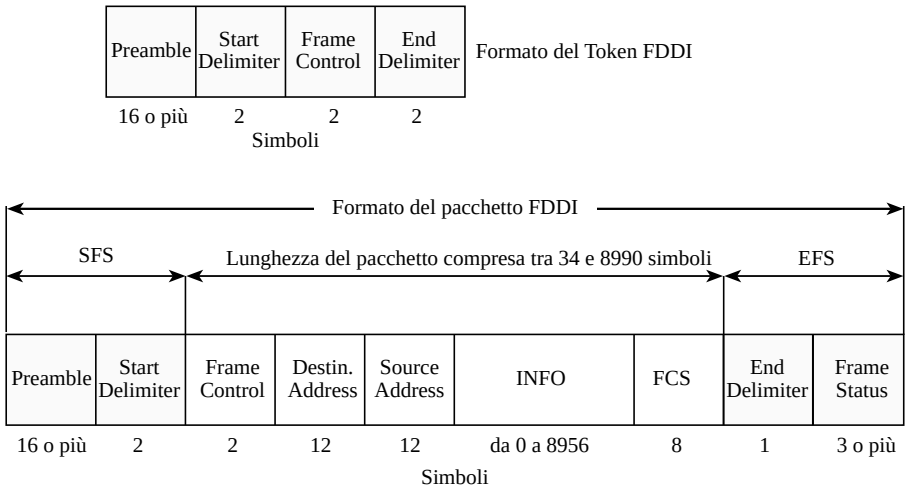
Alla fine di tutte le fasi descritte nell'esempio, nell'anello circola soltanto il token in quanto non c'è nessuna stazione che necessita di trasmettere dei pacchetti.

8.2.2 Ricezione dei pacchetti

Una stazione che non sta trasmettendo un pacchetto ripete tutti i simboli ricevuti alla stazione successiva ed ispeziona continuamente tutto ciò che vede transitare. Ogni stazione compara il campo di destination address dei pacchetti in transito con il proprio indirizzo per verificare se il pacchetto è destinato ad essa o è un pacchetto di multicast o di broadcast; in caso positivo, esegue una copia del pacchetto ed imposta il bit di copied nel campo di *Frame Status* (FS).

8.2.3 Formato del token e del pacchetto

La figura 8.7, mostra il formato del token e del pacchetto FDDI.



Nota: 2 simboli MAC corrispondono ad un ottetto

Fig. 8.7 - Formato del token e del pacchetto.

Il pacchetto è delimitato da:

- lo *Start-of-Frame Sequence* (SFS) che ne indica l'inizio ed è a sua volta composto dal preambolo e dallo start delimiter;
- l'*End-of Frame Sequence* (EFS) che ne indica la fine ed è a sua volta composto dall'end delimiter e dal frame status.

Il *preambolo* (PA: Preamble) è composto da 16 o più simboli di idle ed è collocato in testa sia al token sia al pacchetto; esso è utilizzato dalla stazione ricevente per sincronizzare il proprio clock con quello della precedente stazione trasmittente.

Il campo di *Start Delimiter* (SD) è comune sia al token sia al pacchetto ed è formato da un simbolo J ed un simbolo K (si veda il paragrafo 3.1.3). Esso delimita l'inizio di un token o di un pacchetto.

Il campo di *Frame Control* (FC) è comune sia al token sia al pacchetto e, a seconda del contenuto, indica se è riferito ad un token o ad un pacchetto. Quando si riferisce ad un pacchetto indica se questo è di tipo sincrono (trasmissione video o voce) o asincrono (trasmissione dati) ed in quest'ultimo caso indica se la parte *information* contiene LLC PDU (pacchetti di dati) o MAC PDU (pacchetti di servizio).

Il campo di *frame status* contiene almeno tre simboli che possono assumere i valori R o S:

- il primo si chiama *error detected indicator* ed indica se il pacchetto è errato; esso può essere impostato da una qualunque stazione che rilevi degli errori durante la fase di ripetizione del pacchetto;
- il secondo si chiama *address recognized indicator* ed è impostato dalla stazione che riconosce il destination address come il proprio indirizzo;
- il terzo si chiama *frame copied indicator* ed è impostato dalla stazione che ha copiato il pacchetto.

Nel campo di *Destination Address* (DA) è contenuto l'indirizzo della stazione a cui è destinato il pacchetto, nel campo di *Source Address* (SA) è contenuto l'indirizzo della stazione che ha generato il pacchetto.

Il campo *information* (INFO) può contenere LLC-PDU o MAC-PDU; queste ultime vengono utilizzate principalmente per scopi di gestione della rete, come ad esempio in caso di trasmissione di Claim-PDU e Beacon-PDU.

Il campo FCS (*Frame Check Sequence*) contiene il valore di CRC calcolato sulla base dei campi descritti precedentemente.

8.2.4 Funzione di ripetizione dei simboli

Ogni stazione che non sta trasmettendo pacchetti o emettendo il token ripete le stringhe

di simboli ricevuti alla stazione successiva. Quando una stazione deve trasmettere dei pacchetti attende di ricevere un token, ne modifica il campo Frame Control trasformandolo in un pacchetto e inibisce la ripetizione. Quando la stazione che ha originato un pacchetto riconosce nel campo di source address ricevuto il proprio indirizzo, rimuove dall'anello il pacchetto precedentemente trasmesso e riabilita la ripetizione.

8.2.5 Funzione di rimozione del pacchetto (frame stripping)

Ogni stazione è responsabile di rimuovere dall'anello i pacchetti che ha originato. In realtà, il pacchetto non viene completamente rimosso, ma rimangono dei residui che sono i campi di PA, SD, FC, DA e SA, e questo succede poiché la decisione di rimozione viene presa in base all'osservazione del campo SA e quindi nel frattempo quest'ultimo campo, più quelli precedenti, sono già stati ripetuti. I residui di un pacchetto vengono rimossi quando incontrano una stazione trasmittente.

L'algoritmo previsto dallo standard non è ritenuto efficiente nel caso in cui la stazione FDDI sia un bridge, in quanto il source address del pacchetto non è quello del bridge che sta trasmettendo, bensì quello della stazione trasmittente di un'altra LAN. Per questa ragione è stato sviluppato un algoritmo che si chiama *Frame Content Independent Stripping* (FCIS), basato sulla rimozione dello stesso numero di pacchetti che la stazione ha trasmesso dal momento in cui ha catturato il token. Questo sistema è quindi indipendente dal contenuto dei pacchetti.

8.2.6 Monitoraggio dell'anello (ring monitoring)

Ogni stazione controlla continuamente l'anello per rilevare eventuali condizioni operative non valide che richiedano la re-inizializzazione dell'anello. La re-inizializzazione avviene a seguito della rilevazione di inattività dell'anello o di attività scorretta. L'inattività dell'anello viene rilevata dalla stazione ricevente allo scadere del timer TVX. L'attività scorretta viene rilevata o dalla stazione trasmittente, attraverso il conteggio delle volte in cui è scaduto il timer TRT, o dal processo di SMT.

8.2.7 Accensione delle stazioni

All'accensione ogni stazione entra in una condizione di self-test durante la quale controlla la propria funzionalità. Successivamente inizia un processo di riconoscimento delle stazioni vicine, durante il quale le stazioni si scambiano informazioni circa le connessioni sulle porte. Alla fine di questo processo iniziale si passa alla fase di token claim.

8.2.8 Token claim e inizializzazione dell'anello

Ogni stazione che richiede l'inizializzazione dell'anello incomincia un processo di token claim. Durante questo processo le stazioni trasmettono continuamente dei pacchetti di claim attraverso i quali propongono il proprio valore di TTRT (*Target Token Rotation Timer*) e controllano i pacchetti ricevuti.

Le stazioni comparano la proposta di TTRT ricevuta con il valore da loro proposto. Se il valore ricevuto è inferiore a quello proposto la stazione interrompe la generazione dei pacchetti di claim e ripete quelli ricevuti. Se il valore ricevuto è uguale a quello proposto si comparano gli indirizzi MAC delle stazioni: quella con indirizzo inferiore interrompe la generazione dei pacchetti di claim e ripete quelli ricevuti. Alla fine, una sola stazione continuerà a trasmettere e ricevere i pacchetti di claim, e sarà quella vincente.

La stazione che ha vinto il token claim ha il diritto di inizializzare l'anello: trasmette il valore del TTRT determinato durante il processo di claim ed emette il token. Durante il primo giro di token tutte le stazioni salvano il valore negoziato di TTRT in T_opr; dopo il terzo giro di token l'anello diventa completamente operativo.

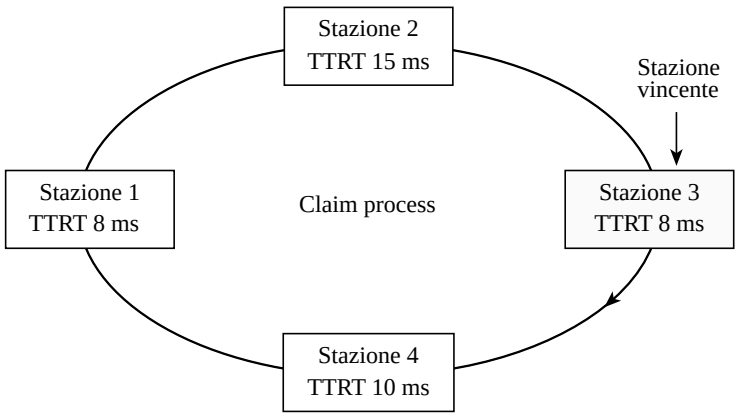


Fig. 8.8 - Esempio di token claim.

La figura 8.8 mostra un esempio di claim del token organizzato nelle seguenti fasi:

- fase 1: tutte le stazioni iniziano a trasmettere i pacchetti di claim;
- fase 2: le stazioni 2 e 4 ricevono un valore di TTRT più basso rispetto al loro e abbandonano il processo di claim, cioè interrompono la trasmissione dei pacchetti di claim e ripetono quelli ricevuti;
- fase 3: la stazione 3 riceve un valore di TTRT identico a quello da essa proposto (8 ms), ma proveniente dalla stazione 1 che ha indirizzo MAC inferiore e continua a trasmettere i pacchetti di claim;

- fase 4: la stazione 1 riceve un valore di TTRT identico a quello da essa proposto, ma dalla stazione 3 che ha indirizzo MAC superiore e abbandona il processo di claim;
- fase 5: la stazione 3 riceve il proprio pacchetto di claim e vince il processo di claim;
- fase 6: la stazione 3 emette il token.

8.2.9 Processo di isolamento dei guasti (beacon process e stuck beacon)

Il motivo per il quale una stazione non riesce a terminare con successo il processo di claiming può derivare da un guasto che causa l'interruzione dell'anello. In questo caso essa inizia un processo di isolamento del guasto trasmettendo in continuazione pacchetti di beacon. Se una stazione riceve un pacchetto di beacon, interrompe il processo di beaconing e ripete il pacchetto ricevuto a quella successiva. Se una stazione riceve il proprio pacchetto di beacon assume che l'anello sia stato ripristinato ed inizia quindi il processo di claim.

Questo meccanismo automatico è sufficiente a ripristinare piccole anomalie momentanee dell'anello. Se invece l'anomalia è seria e persistente si ha una condizione di stuck beacon e si rende necessario l'intervento dei processi controllati dallo SMT, il quale inizia una funzione di *trace*. La funzione di trace induce le stazioni sospette, che sono ai due limiti estremi del guasto, ad abbandonare il ring, entrare in una condizione di bypass ed iniziare il *path test*. Questo serve a verificare il corretto funzionamento di tutti i componenti. Se una stazione fallisce il path test significa che è guasta e quindi si autoesclude dall'anello.

L'esempio riportato nella figura 8.9 riassume le fasi di isolamento di un guasto persistente:

- fase 1: la stazione A è difettosa e non trasmette alla stazione B;
- fase 2: la stazione B inizia un processo di claiming che fallisce e quindi inizia un processo di beacon;
- fase 3: il processo di beacon non è sufficiente a ripristinare l'anello in quanto il guasto è persistente; la stazione B entra quindi in una condizione di stuck beacon ed inizia un processo di trace che trasmette un segnale di MLS (*Master Line State*) sull'anello secondario alla precedente stazione vicina (*upstream neighbor*);
- fase 4: le stazioni A e B abbandonano l'anello ed entrano in uno stato di path test;
- fase 5: il path test indica che la stazione A è guasta, quindi la esclude dall'anello;
- fase 6: la stazione B si riconnette all'anello ed inizia un processo di claim.

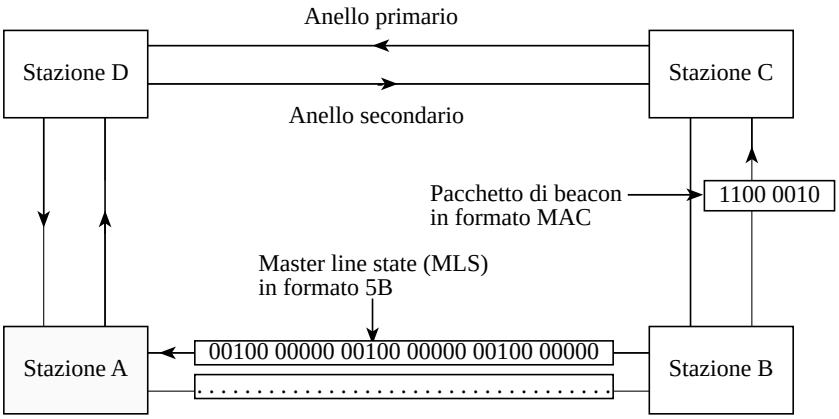


Fig. 8.9 - Esempio di isolamento di un guasto.

La figura 8.10 mostra due diversi esempi di guasto e ripristino dell'anello.

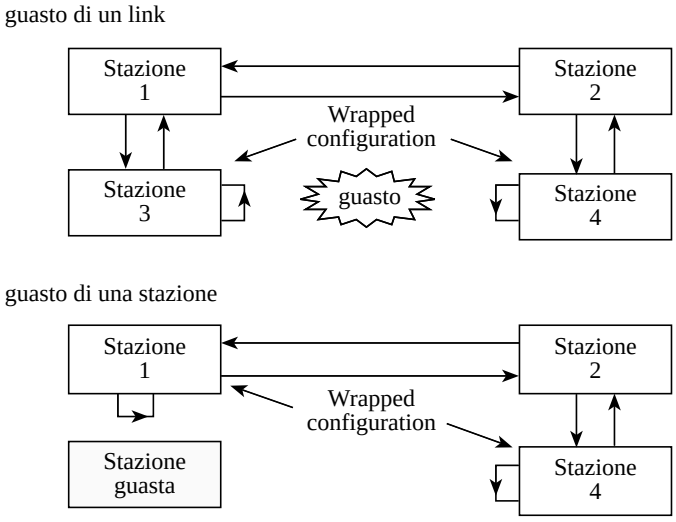


Fig. 8.10 - Esempio di guasti diversi e ripristino.

8.2.10 Parametri, contatori e timer

Tutte le operazioni del livello MAC sono controllate da parametri, contatori e timer che ne definiscono il comportamento.

I parametri principali sono:

- *M_Max* indica il numero massimo delle entità MAC (valore di default 1000). Esso limita il numero massimo di stazioni dell'anello FDDI a 500 in quanto, utilizzando delle stazioni DAS (descritte nel paragrafo 8.5), si hanno due entità MAC per ogni stazione;
- *D_Max* indica il massimo tempo di latenza sull'anello; il valore massimo è 1.773 ms;
- *T_opr* indica il valore del TTRT della stazione che ha vinto il processo di claim token.

Il principale contatore è:

- *Late_Ct* indica il numero di volte che è scaduto il TRT. Viene inizializzato a zero a ogni passaggio del token; se raggiunge il valore 2 determina l'attivazione del processo di claim token; se raggiunge il valore 3 determina l'attivazione del processo di beacon.

I principali timer sono i seguenti:

- *THT (Token Holding Timer)* indica il tempo massimo per il quale una stazione trasmittente può trattenere il token; esso viene inizializzato, quando il token è catturato, al valore di T_opr meno il valore corrente di TRT. THT indica il tempo ancora disponibile per la trasmissione di trame asincrone. Se il valore a cui viene inizializzato è minore o uguale a zero, il token non può essere utilizzato per la trasmissione di trame asincrone e la stazione deve attendere il prossimo passaggio del token per poter trasmettere;
- *TVX (Timer Valid Transmission)* indica il tempo massimo ammesso tra due trasmissioni valide; viene azzerato ad ogni passaggio del token e di pacchetto senza errori; allo scadere si inizia un processo di isolamento dei guasti; il valore minimo ammesso è di 2.5 ms, quello normalmente utilizzato è di 2.62 ms;
- *TRT (Token Rotation Timer)* indica quanto tempo è trascorso dall'ultimo passaggio del token nella stazione. Viene usato per controllare la schedulazione delle operazioni dell'anello durante una condizione normale oppure per rilevare e recuperare delle condizioni di errore. Viene inizializzato a zero ad ogni passaggio del token ed ogni volta che "scade", cioè supera T_opr;
- *TTRT (Target Token Rotation Timer)* indica il tempo di rotazione del token che la stazione propone durante il processo di claiming (normalmente questo valore è di 8 ms); il valore è compreso tra altri due valori che sono: *T_Min*, il cui valore massimo ammesso è 4 ms, e *T_Max* il cui valore minimo ammesso è 165 ms.

8.3 FUNZIONI DELL'ELEMENTO PHY

Le funzioni principali dell'elemento PHY sono le seguenti:

- la codifica (e decodifica) NRZ *(Non Return to Zero)* e NRZI *(Non Return to Zero Inverted on one)*, descritte nel paragrafo 3.1.2;
- la codifica e decodifica 4B/5B (paragrafo 3.1.3);
- la determinazione degli stati della linea (line states) che serve allo SMT per verificare e mantenere l'integrità dell'anello. Essi sono: *Quiet Line State* (QLS), *Master Line State* (MLS), *Halt Line State* (HLS), *Active Line State* (ALS), *Noise Line State* (NLS) *e Idle Line State* (ILS). Quest'ultimo è particolarmente importante perché serve a stabilire e mantenere la sincronizzazione del clock sulla stazione ricevente.

Nella parte PHY rientrano una serie di circuiti responsabili di determinate funzioni che ricoprono una particolare importanza per il corretto funzionamento dell'anello FDDI.

Il circuito di elasticity buffer è utilizzato da ogni stazione per compensare le differenze di clock. Esso è di fatto un registro FIFO (*First-In First-Out*) in cui la minima capacità richiesta è di 5 bit.

Il circuito di smoothing assorbe il surplus di bit di preambolo e li ridistribuisce nei preamboli più corti in modo da manternerli entro i limiti di tolleranza.

8.4 LE FUNZIONI DELL'ELEMENTO SMT

Ci sono tre famiglie di funzioni che sono:

- il *PCM (Physical Connection Management)* che si occupa dell'inserzione, rimozione o condizione di bypass di una stazione;
- il *RMT (Ring Management)* che si occupa della gestione dell'anello;
- il *CFM (Configuration Management)* tramite il quale è possibile intervenire sui parametri di configurazione della stazione.

La figura 8.11 mostra lo schema logico delle principali funzioni di SMT.

Periodicamente lo SMT si occupa di inviare i pacchetti di notifica delle stazioni vicine chiamati NIF (*Neighbor Information Frame*) che sono usati dalla stazione per annunciare il suo indirizzo ed una sua descrizione.

Nel caso si sospetti un guasto della stazione, essa entra in uno stato di path test.

In caso di guasto persistente dell'anello, lo SMT si occupa della funzione di trace che serve ad isolare il guasto e a ripristinare l'anello (si veda il paragrafo 8.2.9).

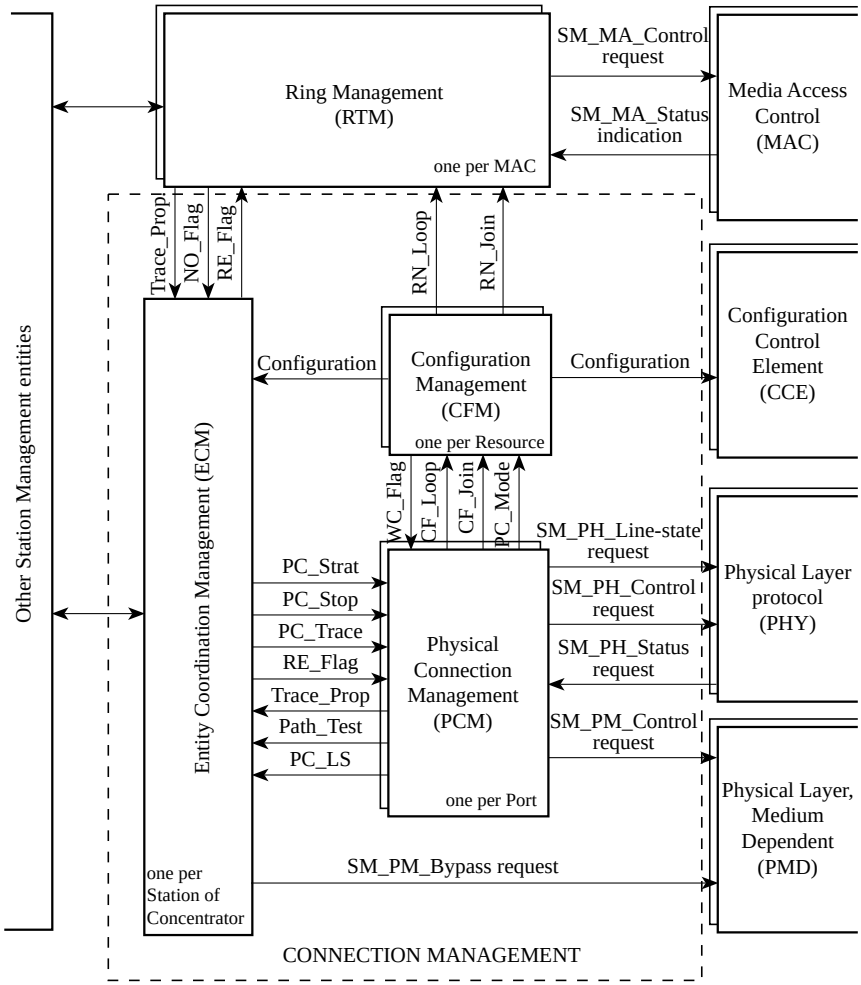


Fig. 8.11 - Schema logico delle principali funzioni di SMT.

8.5 TIPI DI STAZIONI

Esistono tre tipi di stazioni FDDI:

- la stazione *DAS (Dual Attachment Station)* che si collega direttamente all'anello primario e a quello secondario, può disporre di un relé ottico di bypass, offre un'ottima tolleranza ai guasti, ma ha costi elevati (figura 8.12);

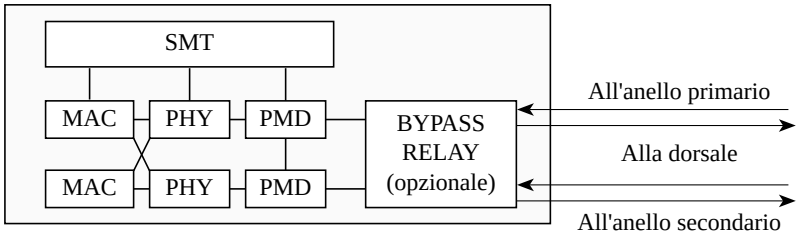


Fig. 8.12 - Stazione DAS.

- la stazione *SAS (Single Attachment Station)* che si collega all'anello tramite il concentratore DAC (Dual Attachment Concentrator), fornisce una sola connessione all'anello FDDI, delega parte del controllo dei guasti al concentratore, ha costi relativamente bassi ed è l'unica soluzione possibile nel caso che la stazione utilizzi cavi STP o UTP (figura 8.13);

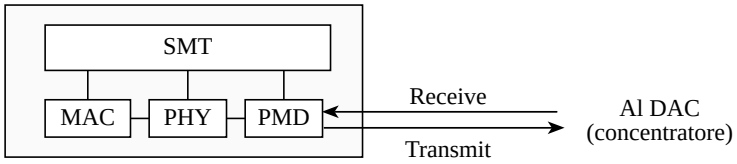


Fig. 8.13 - Stazione SAS.

- la stazione *DAC (Dual Attachment Concentrator)* che è un concentratore attivo che permette la connessione di stazioni SAS all'anello e controlla la topologia della rete, inserendo o rimuovendo le stazioni ad essa connesse tramite l'uso di switch elettronici; ogni elemento PHY è gestito separatamente dall'elemento SMT (figura 8.14). Il DAC può essere usato come radice di un albero di stazioni.

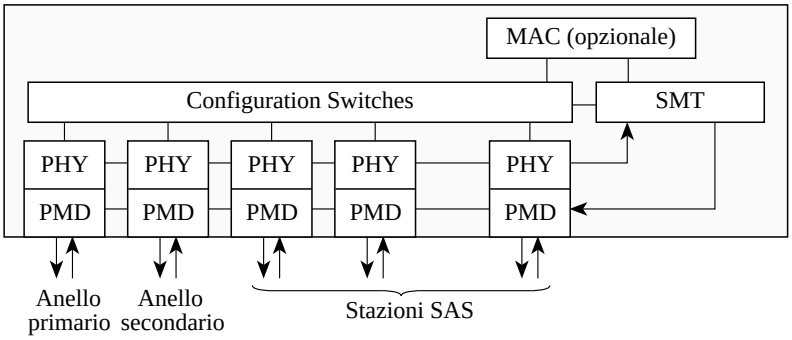


Fig. 8.14 - Concentratore DAC.

8.6 GLI STANDARD PMD

8.6.1 Lo standard ANSI X3.166 - ISO/IEC 9314-3

Questo è il primo standard PMD approvato ed è anche il più diffuso e conosciuto. Si basa sull'utilizzo della fibra ottica multimodale 62.5/125 e dei LED che lavorano in seconda finestra (1300 nm). Esso stabilisce le caratteristiche della fibra ottica e dei componenti del cablaggio.

La fibra ottica deve rispondere ai requisiti dello standard EIA/TIA 568 o ISO/IEC 11801 (si veda il capitolo 4).

Il link costituito dalla fibra ottica più tutti gli eventuali connettori, giunti o splice, non deve attenuare più di 11 dB.

La distanza massima ammessa tra due stazioni FDDI è di 2 Km; questa distanza massima può essere ridotta qualora l'attenuazione globale del link superi gli 11 dB.

Il connettore MIC (*Medium Interface Connector*) utilizzato dagli apparati FDDI è il connettore duplex ST riportato nella figura 8.15.

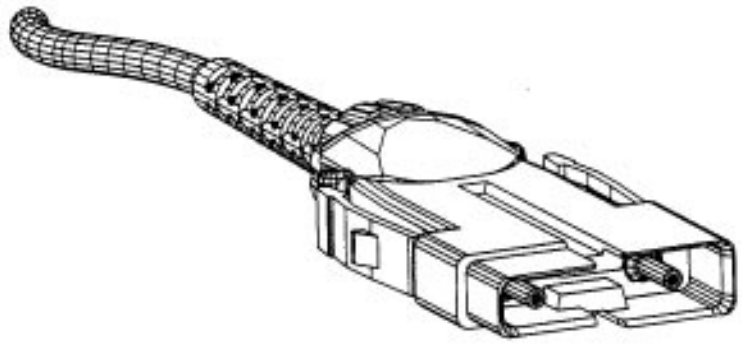


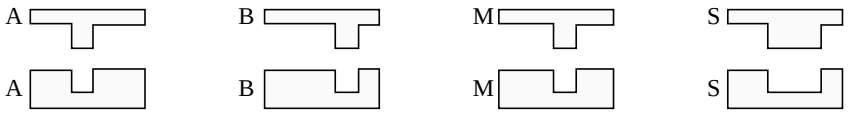
Fig. 8.15 - Connettore FDDI.

Esso possiede una chiave d'inserzione configurabile dall'utente che serve a specializzare il tipo di connessione e, a seconda delle posizioni, può essere usata per l'inserzione nella porta A, B, M, S di una stazione (figura 8.16).

Il bypass switch ottico è opzionale e serve a prevenire sezionamenti multipli dell'anello a seguito dello spegnimento di alcune stazioni. Esso deve avere un'attenuazione massima di 2.5 dB, sia in condizione normale sia in condizione di bypass. Il bypass switch è basato su un principio elettromeccanico a specchi e quando viene a mancare la tensione di alimentazione commuta in posizione di bypass. Esso non è

quasi mai utilizzabile a causa dell'elevata attenuazione.

La funzione dei bypass switch ottici viene meglio effettuata dai concentratori DAC, i quali rimuovono in modo elettronico le stazioni SAS che vengono spente.



Connector keying:
MIC A Primary in/secondary out-DAS A port
MIC B Primary out/secondary in-DAS B port
MIC M Concentrator M port
MIC S SAS S port

Fig. 8.16 - Chiavi d'inserzione dei connettori MIC.

8.6.2 Lo standard ANSI X3.184

Questo standard, chiamato SMF-PMD (*Single Mode Fiber PMD*), si basa sull'utilizzo della fibra ottica monomodale e fa uso di laser che lavorano in seconda finestra (1300 nm). Esso stabilisce le caratteristiche della fibra ottica e dei componenti del cablaggio.

La fibra ottica monomodale deve soddisfare i seguenti principali requisiti:

- diametro del core da 8.2 a 10.5 μm;
- diametro del cladding 125 μm ± 2;
- attenuazione massima 0.4 dB/Km;
- non circolarità del cladding 2% max;
- assenza di dispersione della lunghezza d'onda da 1300 a 1322 nm;
- dispersione dello slope ≤ 0.095 ps/(nm^2 Km);
- errore di concentricità tra core e cladding ≤ 1 μm;
- cut-off della lunghezza d'onda del cavo ≤ 1270 nm.

Lo standard definisce due classi di lavoro per i laser emettitori chiamati AOI (*Active Output Interface*) e per i ricevitori chiamati AII (*Active Input Interface*). Si possono utlizzare componenti di entrambe le classi in tutte le possibili combinazioni.

I trasmettittori e di ricevitori devono avere le caratteristiche riportate nella tabella 8.1.

	Descrizione del parametro	Categoria I		Categoria II		Unità di misura
		Min	Max	Min	Max	
A	Central wavelength	1270	1340	1290	1330	nm
O	RMS spectral width	--	15	--	5	nm
I	Average power	-20	-14	-4	0	dBm
A	Central wavelength	1270	1340	1290	1330	nm
I	Average power	-31	-14	-37	-15	dBm
I						

Tab. 8.1 - Caratteristiche dei laser.

A seconda delle combinazioni dei trasmettittori e dei ricevitori laser si possono avere i seguenti valori di perdita nel link:

- AOI_I con AII_I da 0 a 10 dB;
- AOI_I con AII_II da 1 a 16 dB;
- AOI_II con AII_I da 14 a 26 dB;
- AOI_II con AII_II da 15 a 32 dB.

Quando il valore minimo di perdita è superiore a zero, sta ad indicare la minima attenuazione del link necessaria per evitare la saturazione del ricevitore; in taluni casi, se la tratta è corta, si rende necessario inserire un attenuatore ottico.

Con trasmettitori e ricevitori di classe I si può avere una distanza massima di circa 10 Km, in quanto la fibra introduce un'attenuazione di 4 dB ed ulteriori 4 dB vanno normalmente persi tra i connettori e i cavetti di permutazione; si consideri infine che un cavo in fibra ottica viene fornito normalmente in pezzature da 2 Km e che ogni giunzione introduce una perdita di circa 0.2 dB.

Il connettore utilizzato è molto simile al connettore MIC FDDI del precedente standard; cambiano soltanto le chiavette d'inserzione per evitare di collegare una porta per fibra multimodale con una di tipo monomodale.

Alcuni costruttori, ad esempio la Digital, preferiscono utilizzare i connettori FC-PC poiché sono più adatti ad applicazioni con fibre monomodali, sono inoltre lappati con un angolo di circa 8 gradi e presentano un valore di return loss migliore dei connettori MIC. Il return loss rappresenta la potenza ottica riflessa, che è particolarmente dannosa per gli emettitori laser.

8.6.3 La bozza di standard ANSI X3.237

Questa bozza di standard LCF-PMD (*Low Cost Fiber PMD*) si basa sull'utilizzo della fibra ottica multimodale 62.5/125 e dei LED che lavorano in seconda finestra (1300 nm) come il primo standard, ma a differenza di questo utilizza componentistica di basso costo e accetta tutti i tipi di fibra multimodale graded index. Questo standard stabilisce le caratteristiche della fibra ottica e dei componenti del cablaggio.

La fibra ottica deve avere come requisito elettrico minimo una banda passante di almeno 500 MHz · Km.

Il link costituito dalla fibra ottica, più tutti gli eventuali connettori, giunti o splice, non deve attenuare più di 7 dB.

La distanza massima ammessa tra due stazioni FDDI è di 500 m e può essere ridotta qualora l'attenuazione globale del link superi i 7 dB.

I connettori utilizzati sono gli SC duplex.

8.6.4 La bozza di standard ANSI TP-PMD

Questa bozza di standard TP-PMD (*Twisted Pair PMD*) si basa sull'utilizzo di cavi STP e UTP e permette soltanto connessioni di stazioni SAS al concentratore DAC.

La distanza massima consentita è di 100 m tra il concentratore e la stazione, di cui 90 m per il cablaggio e 10 m per i cavetti di permutazione.

Lo standard utilizza la codifica MLT-3 per ridurre l'attenuazione e, nel caso di utilizzo di cavi UTP, anche gli effetti di emissione di radiofrequenze (EMC). La funzione di trasmissione riceve dal PHY delle stringhe di dati codificati secondo il metodo standard NRZI, li converte in NRZ, poi esegue la codifica MLT-3 e li trasmette sul mezzo trasmissivo. La funzione di ricezione riceve dal mezzo trasmissivo delle stringhe di dati codificati secondo il metodo MLT-3, li decodifica, ottiene dei dati codificati in NRZ e poi li converte in NRZI per poterli presentare al PHY.

I connettori permessi sono i seguenti:

- STP-MIC per cavo STP: è un connettore DB9 conforme alle specifiche EIA/TIA 574 del 1990;
- UTP-MIC per cavo UTP: è un connettore RJ45 conforme alle specifiche EIA/TIA TSB 40.

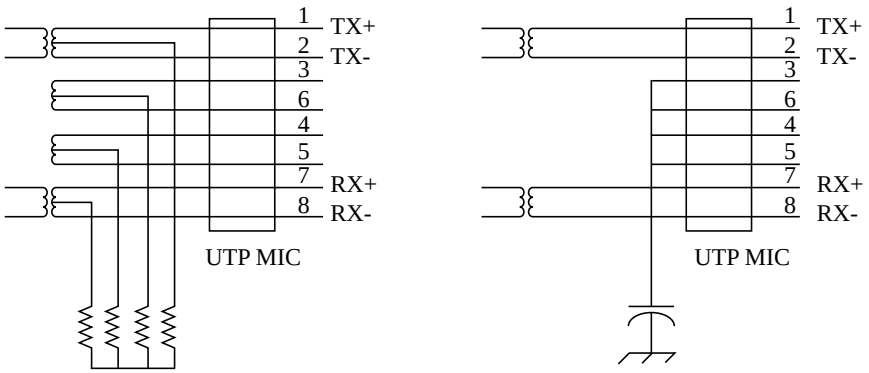
Il cavo UTP deve essere di categoria 5, il cavo STP deve rispecchiare le caratteristiche del cavo di tipo 1 IBM. Nel caso di utilizzo di cavo UTP tutta la componentistica deve essere di categoria 5 e l'installazione deve essere eseguita

rispettando le specifiche di categoria (si veda il capitolo 4 ed in particolare le specifiche EIA/TIA 568, TSB 36 e 40 e quelle ISO/IEC 11801).

Per migliorare le caratteristiche di non emissione di radiofrequenze (EMI) nel caso di utilizzo di cavi UTP, lo standard propone due tecniche di terminazione:

- la prima tecnica richiede una terminazione resistiva all'interno della stazione;
- la seconda tecnica impone di collegare alla massa della stazione le coppie inutilizzate.

La figura 8.17 mostra queste due tecniche di terminazione.



Terminazione resistiva all'interno della stazione

Terminazione delle coppie inutilizzate alla massa della stazione

Fig. 8.17 - Terminazione delle coppie inutilizzate.

8.7 REGOLE DI CONFIGURAZIONE

8.7.1 Topologie

Una rete FDDI può essere realizzata secondo le seguenti topologie:

- completamente ad anello, utilizzando soltanto stazioni di tipo DAS;
- completamente a stella o ad albero, utilizzando soltanto concentratori DAC e stazioni SAS;
- con una dorsale ad anello che interconnette i concentratori e con cablaggio stellare dal concentratore alle stazioni. Questa topologia è quella più usata.

La figura 8.18 mostra un esempio di topologia stellare ad albero.

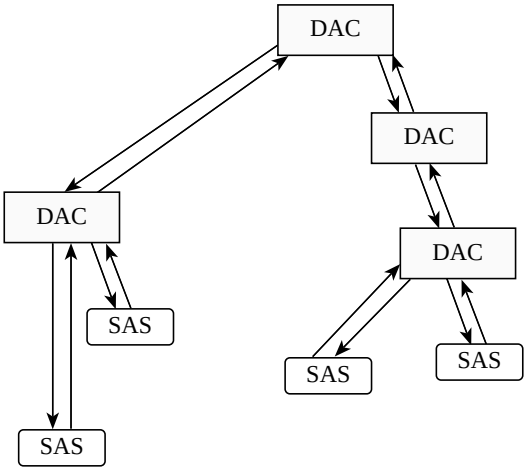


Fig. 8.18 - Topologia stellare ad albero.

La figura 8.19 mostra una topologia avente la dorsale ad anello e la distribuzione alle stazioni di tipo stellare.

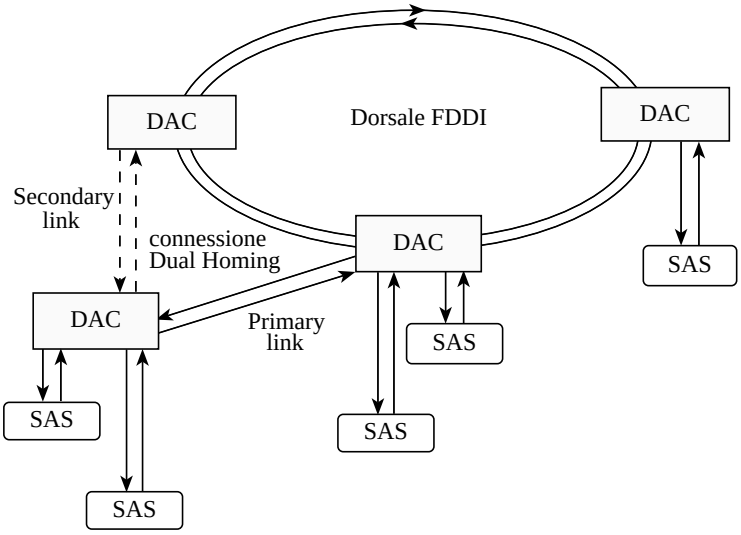


Fig. 8.19 - Dorsale ad anello e distribuzione a stella.

Per aumentare l'affidabilità dei sistemi stellari si adotta una tecnica chiamata *dual homing* che consiste nel connettere il concentratore di secondo livello a porte diverse

di concentratori diversi, in cui una connessione è primaria ed attiva e l'altra è secondaria ed in stato di backup caldo.

La figura 8.20 mostra le possibili combinazioni e connessioni tra i concentratori e le stazioni indicando i tipi di porte utilizzate.

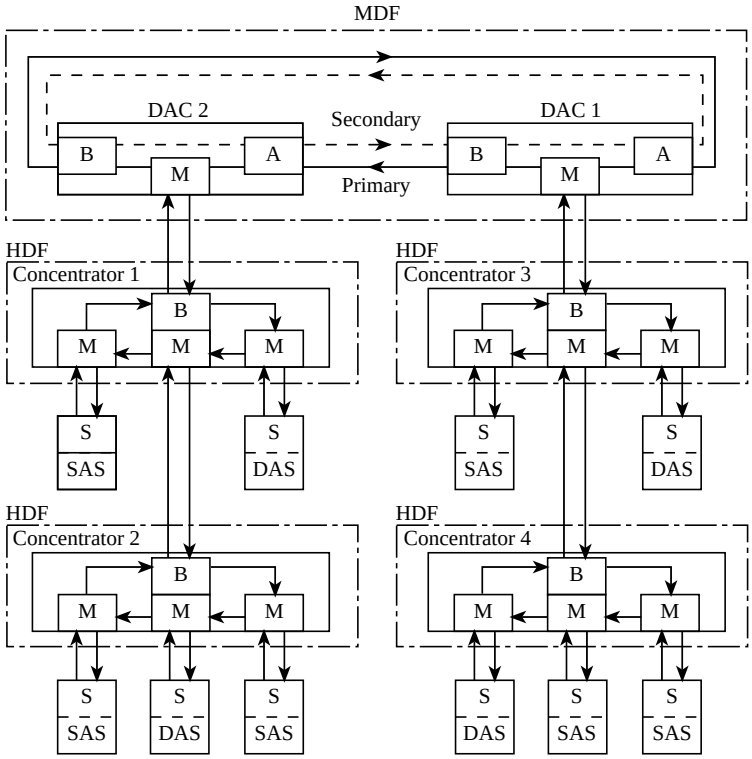


Fig. 8.20 - Possibili connessioni fra le stazioni FDDI.

8.7.2 Regole di configurazione

La distanza massima percorribile da un segnale è di 200 Km ed include anche il percorso dell'anello secondario utilizzato in caso di guasto. Ne consegue che, se in un anello si utilizzano soltanto stazioni DAS, la circonferenza massima è di 100 Km. Se si usano i concentratori e le stazioni SAS bisogna calcolare il percorso peggiore in caso di guasto, che non deve superare i 200 Km.

In una rete FDDI si possono avere al massimo 1000 connessioni fisiche e, considerando che una stazione DAS ha 2 connessioni fisiche (porta A e porta B), ne

consegue che, se in un anello si utilizzano soltanto stazioni DAS, il numero massimo di stazioni è 500. Se si utilizzano stazioni SAS si hanno due connessioni fisiche per link, di cui una connessione alla porta S della stazione e una connessione alla porta M del concentratore. Inoltre per ogni concentratore ci sono tipicamente due connessioni fisiche sull'anello primario (porta A e porta B); in questo caso il numero delle connessioni fisiche è uguale a: 2 x DAC + 2 x SAS. Il risultato del calcolo delle connessioni fisiche deve essere minore o uguale a 1000.

La distanza massima tra due stazioni dipende dal tipo di PMD utilizzato per cui si ha:

- PMD standard per fibra ottica multimodale: è ammessa un'attenuazione massima di 11 dB sul link e se questa condizione è soddisfatta la distanza massima è di 2 Km;
- LCF-PMD standard per fibra ottica multimodale a basso costo: è ammessa un'attenuazione massima di 7 dB sul link e se questa condizione è soddisfatta la distanza massima è di 500 m;
- SMF-PMD standard per fibra ottica monomodale: la distanza dipende dalle combinazioni delle due classi di emettitori/ricevitori utilizzati, ma comunque, nel caso di peggiore combinazione, si possono coprire distanze di 10 Km e, nel caso di migliore combinazione, si possono coprire distanze di 50 Km;
- TP-PMD standard per cavi UTP e STP: la distanza massima tra la stazione SAS ed il concentratore è di 100 m.

BIBLIOGRAFIA

[1] Fiber Distribuited Data Interface, System Level Description, document nr. EK-DFSLD-SD-002, Digital Equipment Corporation.

[2] FDDI BASIC, Standards ANSI X3.139, X3.148, X3.166, X3.229, 1994 Global Engineering Documents, ISBN: 1-57053-002-5.

[3] FDDI PMD Set, Standards ANSI X3.166, X3.184, X3.237 and TP-PMD, 1994 Global Engineering Documents, ISBN: 1-57053-004-1.

9

LA RETE DQDB E LO STANDARD IEEE 802.6

9.1 INTRODUZIONE

La problematica delle reti metropolitane (MAN: *Metropolitan Area Network*) è sempre stata di interesse sia per i costruttori di elaboratori e di apparati di telecomunicazione, sia per le PTT nazionali.

Vari sono stati gli sforzi nel tentativo di giungere ad uno standard per le MAN. Tra questi ricordiamo la proposta della Burroughs basata su una tecnologia slotted ring, poi abbandonata, e la proposta sviluppata dalla University of Western Australia con il contributo della Telecom Australia per una rete detta QPSX (*Queued Packet and Synchronous Exchange*).

Questa proposta è alla base dello standard IEEE 802.6 *Distributed Queue Dual Bus* (DQDB) *Subnetwork of a Metropolitan Area Network* che ha ottenuto un largo consenso dalle compagnie telefoniche nord-americane (BOC:*Bell Operating Company*) ed una più tiepida accoglienza in Europa, dove è stato adottato da Inghilterra, Germania e Italia, e rifiutato dalla Francia.

Lo standard 802.6 è stato approvato dal comitato IEEE alla fine del 1990 e dal comitato ANSI nella prima metà del 1991.

DQDB è l'unico standard IEEE 802 (figura 9.1) che sia stato riconosciuto dal CCITT ed utilizzato in reti pubbliche.

Lo standard DQDB si occupa in particolare del sottolivello MAC del livello 2, in quanto a livello Fisico si adottano standard consolidati nell'ambito delle reti di telecomunicazioni pubbliche. Lo standard tratta una singola sottorete DQDB e la connessione di un insieme di sottoreti DQDB a formare una MAN. Questa ha numerose affinità logiche con una LAN estesa.

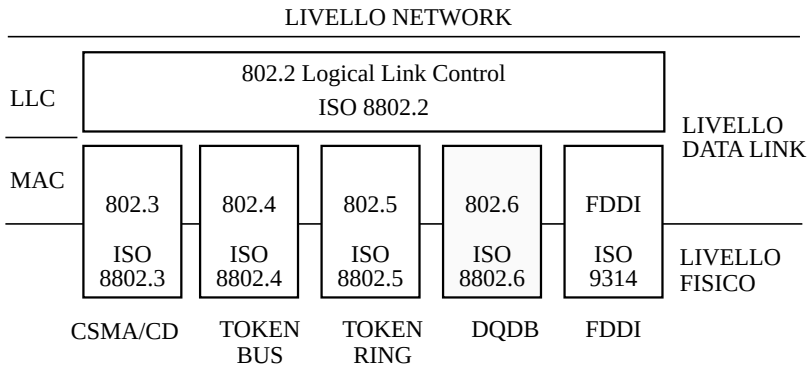


Fig. 9.1 - Relazioni tra i livelli OSI e DQDB.

L'interconnessione tra le sottoreti DQDB all'interno di una MAN si può realizzare utilizzando bridge multiporta, router o gateway (figura 9.2). Il bridge multiporta per l'interconnessione di sottoreti DQDB non è un normale bridge IEEE 802.1D, ma è conforme alle specifiche dei bridge remoti per le MAN che sono oggetto di una bozza di standard denominata IEEE 802.6F-D5 e datata 1993.

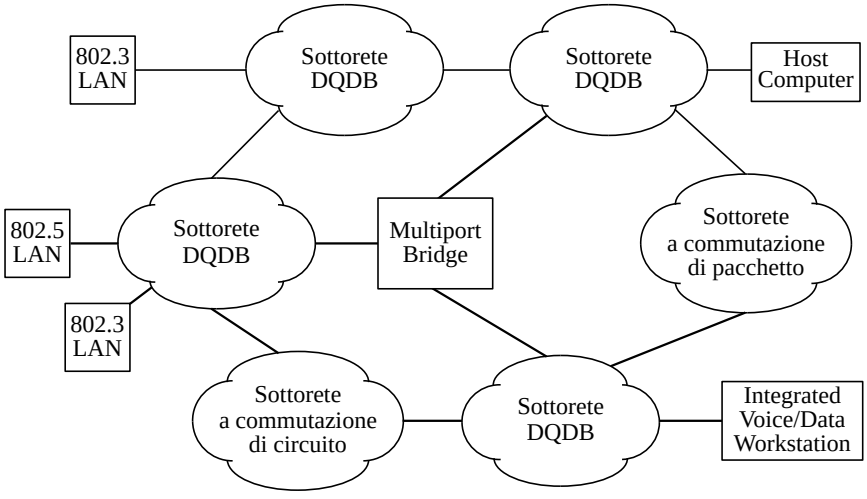


Fig. 9.2 - Metropolitan Area Network.

9.2 IL LIVELLO MAC

9.2.1 Metodo di accesso

Il metodo di accesso, come la sigla DQDB ricorda, si basa su un algoritmo distribuito di accodamento delle richieste di trasmissione, detto anche coda distribuita. In pratica, quando una stazione DQDB deve trasmettere, accoda la sua richiesta di trasmissione sulla rete e, quando saranno terminate le trasmissioni delle stazioni che hanno fatto richiesta precedentemente, la stazione potrà trasmettere. La coda delle richieste è unica per tutte le stazioni ed è gestita in modo distribuito.

Una sottorete DQDB è realizzata tramite due bus seriali che trasmettono i dati in direzioni opposte (figura 9.3). Sui due bus i nodi vengono connessi tramite le *Access Unit* (AU) che realizzano il protocollo DQDB.

I nodi che si trovano ai due estremi del doppio bus prendono il nome di *head-of-bus*. Essi sono il punto di generazione del flusso di dati per un bus (*start of data flow*) ed il punto di terminazione del flusso di dati per l'altro bus (*end of data flow*).

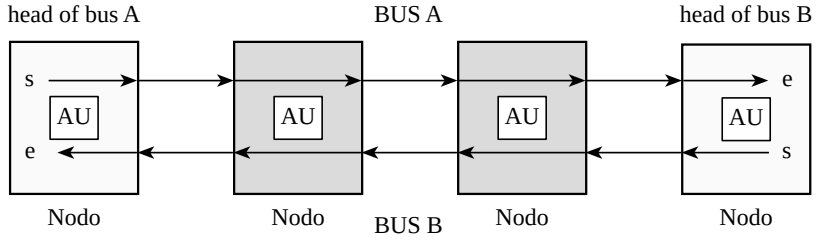


Fig. 9.3 - Sottorete DQDB: topologia open bus.

Una sottorete DQDB può essere configurata con due topologie:

- *open bus*. Si tratta di un doppio bus con le estremità aperte (figura 9.3). In caso di guasto la sottorete si divide in due sottoreti che rimangono isolate;
- *looped bus*. Si tratta di un doppio bus richiuso ad anello che offre buone caratteristiche di tolleranza ai guasti (figura 9.4).

Nella topologia looped bus l'head-of-bus A e l'head-of-bus B sono presenti all'interno nello stesso nodo. In caso di rottura fisica di una connessione, i due nodi posti agli estremi del guasto diventano le due nuove head-of-bus dei bus e la sottorete si riconfigura quindi in modalità open bus (figura 9.5).

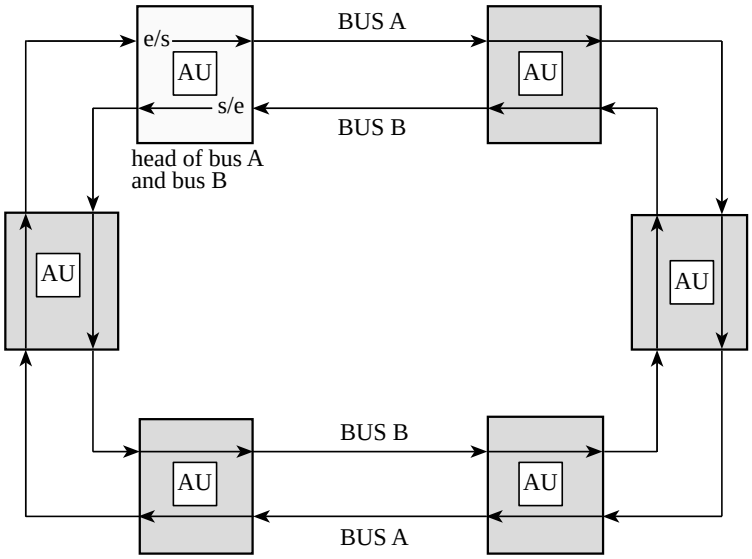


Fig. 9.4 - Sottorete DQDB: topologia looped bus.

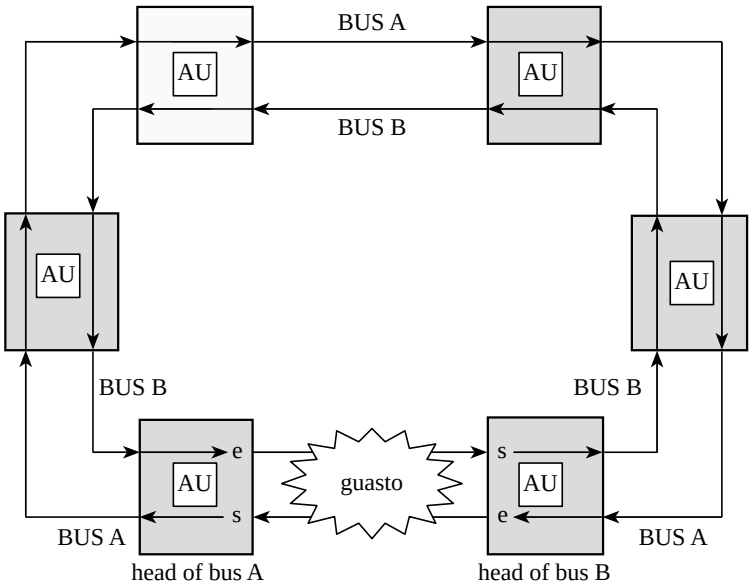


Fig. 9.5 - Riconfigurazione di un looped bus a seguito di un guasto.

Ogni nodo ha una *Access Unit* (AU) che realizza le funzionalità del protocollo DQDB e si connette ai bus A e B tramite due connessioni: una di read (lettura) e una di write (scrittura). La scrittura o trasmissione dei dati sul bus avviene tramite un OR logico con i dati provenienti dal nodo precedente (figura 9.6).

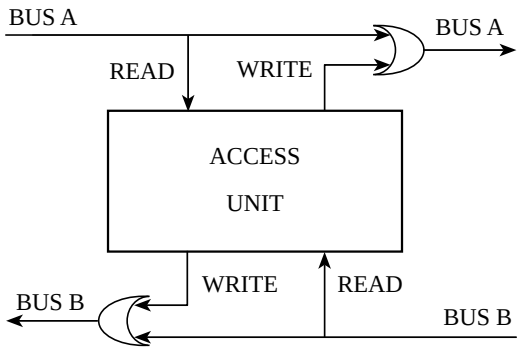


Fig. 9.6 - Connessione di una Access Unit.

Si noti che la connessione di lettura o ricezione dei dati è messa sequenzialmente prima di quella di scrittura, perciò la Access Unit può copiare i dati, modificarli se ciò è permesso dal MAC, ma non rimuoverli.

Le Access Unit sono connesse ai bus in modo non condizionante, per cui possono essere inserite o rimosse senza conseguenze funzionali per la sottorete DQDB. Una Access Unit che si guasta, senza comportare danni distruttivi sul bus, non compromette il funzionamento della sottorete.

Le uniche unità che, a seguito di una rimozione dal doppio bus o di un guasto non distruttivo, condizionano il funzionamento della sottorete sono gli head-of-bus, in quanto si occupano di generare e terminare i flussi di dati.

La determinazione del nodo *head-of-bus* viene effettuata dalle DQDB LME (*Layer Management Entities*), cioè dalle unità di gestione dei nodi DQDB che si scambiano opportuni messaggi di gestione.

9.2.2 Servizi della sottorete DQDB

I servizi forniti dalla sottorete DQDB sono di tre tipi:

- servizio isocrono (ISU: *Isochronous Service User*) per trasporto di informazioni che necessitano di un trasferimento sincrono a velocità costante, quali la voce e le immagini digitali;

- servizio MAC non connesso: tramite delle MSDU (*Mac Service Data Unit*) di lunghezza variabile si trasportano dati tra le entità LLC, senza stabilire una connessione tra le entità MAC; il protocollo LLC potrà naturalmente essere connesso o non connesso;
- servizio connesso di tipo asincrono per trasporto di dati tra entità diverse da quelle LLC.

L'unità base per il trasferimento di informazioni è lo *slot*. Gli head-of-bus generano in continuazione degli slot che possono essere utilizzati dalle Access Unit. I criteri per arbitrare l'utilizzo di tali slot, cioè per accedere al doppio bus, sono due (figura 9.7):

- *Pre-Arbitrated* (PA) utilizzato per fornire i servizi isocroni. Gli slot PA vengono riservati in fase di generazione per essere utilizzabili solo da determinate Acces Unit;
- *Queued Arbitrated* (QA) utilizzato per fornire i servizi non isocroni. Gli slot QA vengono generati vuoti e possono essere utilizzati da tutte le Access Unit secondo le modalità del protocollo MAC a coda distribuita.

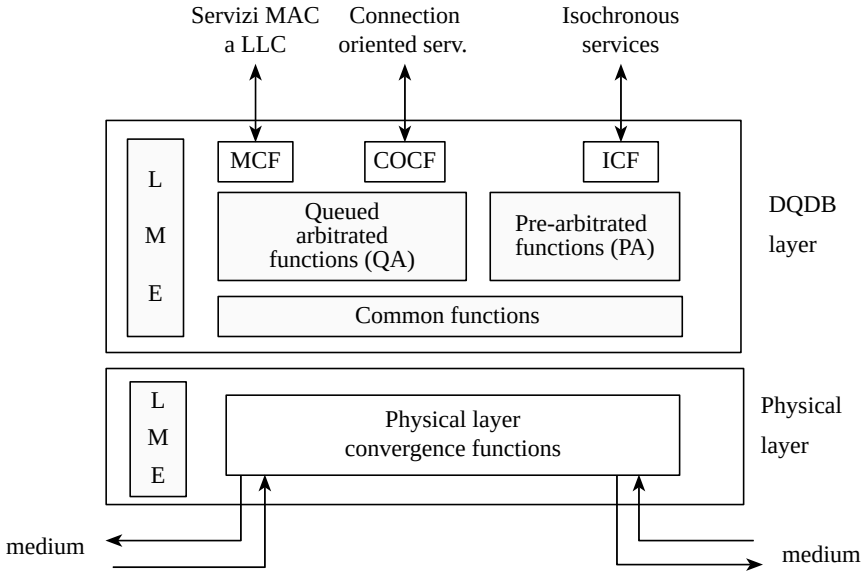


Fig. 9.7 - Schema logico a livelli di un nodo DQDB.

9.2.3 Unità base di trasferimento delle informazioni (slot)

Lo slot può contenere dati o informazioni di gestione. La figura 9.8 mostra il formato dello slot.

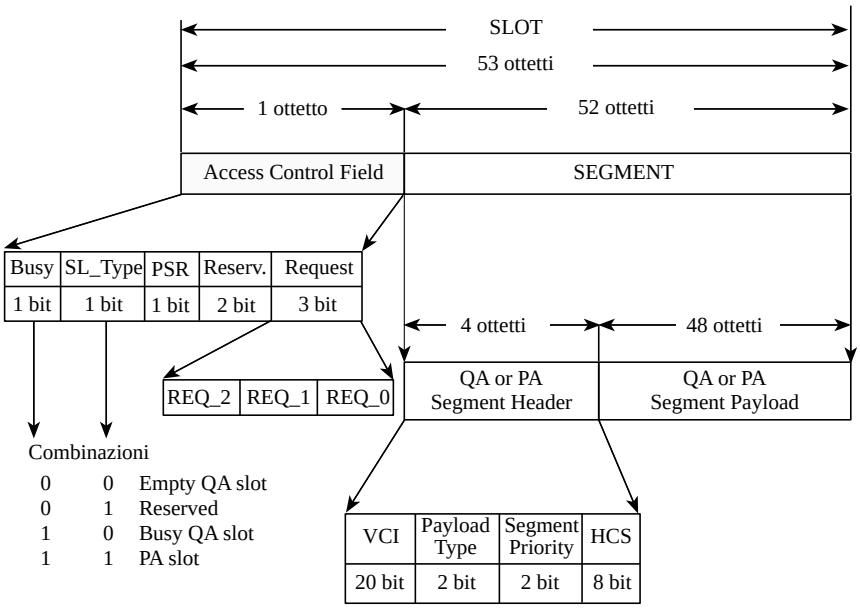


Fig. 9.8 - Formato dello slot.

Si noti che lo slot ha lunghezza fissa pari a 53 byte ed è stato progettato per avere un elevato grado di compatibilità con la cella ATM (si veda paragrafo 19.2).

Gli slot vengono generati in continuazione su entrambi i bus dai nodi head-of-bus. All'atto della generazione sono vuoti (non contengono dati) e possono essere riempiti dalle Access Unit dei nodi che hanno necessità di trasferire informazioni.

Lo slot è formato da due parti principali: l'*Access Control Field* (ACF) ed il *segmento*.

I bit dell'ACF controllano l'accesso allo slot ed in particolare:

- i due bit *Busy* e *SL_Type* definiscono lo stato dello slot che può essere:
  - slot QA vuoto;
  - slot QA occupato;
  - slot PA;
- i tre bit di *request* indicano una richiesta di accesso QA ad uno dei tre livelli di priorità disponibili.

I segmenti possono essere di tipo PA, quando sono riferiti ad uno slot di tipo *pre-arbitrated*, o di tipo QA quando sono riferiti ad uno slot di tipo *queued arbitrated*.

Il segmento è suddiviso in due ulteriori campi:

- il *segment header* contiene le informazioni relative al payload e al tipo di connessione;
- il *segment payload* è il campo dati, lungo 48 ottetti.

Il segment header è a sua volta composto da:

- *VCI (Virtual Channel Identifier)*, che identifica il canale virtuale a cui appartiene il segmento. Il servizio MAC non connesso fornito al livello LLC è identificato tramite il VCI con tutti i bit a uno;
- *Payload Type e Segment Priority*, che hanno sempre valore zero; altri valori saranno oggetto di definizioni future;
- *HCS (Header Check Sequence)*, che è un CRC calcolato sull'header.

Durante il normale funzionamento tutte le stazioni sono sincronizzate su un'unica sorgente che genera il tempo base di slot (*slot timing*) per una sottorete DQDB. Questo serve a garantire che tutti nodi della sottorete identifichino correttamente la tempistica degli slot.

9.2.4 Metodo di accesso Queued Arbitrated (QA)

Questo metodo di accesso utilizza gli slot di tipo QA e fornisce un accesso deterministico per i servizi di trasferimento dati.

Il protocollo utilizza i bit di busy e SL_Type per verificare la disponibilità dello slot e il campo request per richiedere un accesso ad un dato livello di priorità.

Ogni nodo deve tenere conto di quali altri nodi sono raggiungibili tramite il bus A e quali tramite il bus B. Lo standard IEEE 802.6 non definisce la metodologia per fare ciò, ma suggerisce di utilizzare le tecniche già adottate con successo dallo standard IEEE 802.1D relativamente alla gestione delle tabelle di instradamento dei MAC bridge (si veda paragrafo 10.6).

Il nodo che vuole trasmettere decide, in funzione dell'indirizzo di destinazione, se utilizzare il bus A o il bus B, e il bus scelto diventa il suo *forward bus*, mentre l'altro bus diventa il suo *reverse bus*, per quella trasmissione.

Con riferimento all'esempio di figura 9.9 supponiamo che il nodo X debba trasmettere un segmento al nodo Z. Per detta trasmissione il forward bus di X è il bus A, mentre il reverse bus di X è il bus B.

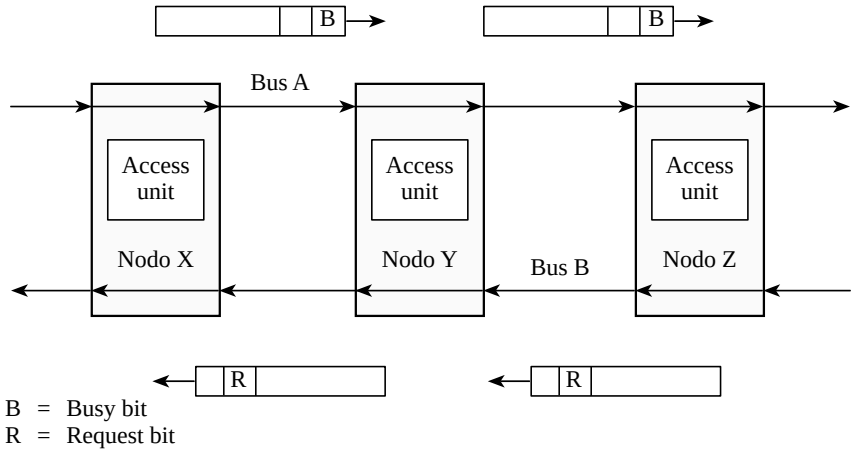


Fig. 9.9 - Esempio di Forward e Reverse BUS.

Il nodo non può trasmettere utilizzando il primo slot QA libero sul forward bus, in quanto questo avvantaggerebbe i nodi vicini allo head-of-bus a danno di quelli più lontani, ma deve prima prenotare la trasmissione usando il reverse bus. Questo equivale a gestire una coda di prenotazioni distribuita.

Solo quando saranno state servite le prenotazioni precedenti nella coda, il nodo potrà trasmettere. A tal fine ogni nodo mantiene un conteggio del numero di prenotazioni dei nodi successivi sul forward bus non ancora servite, come differenza tra il numero di prenotazioni che ha visto transitare sul reverse bus e il numero di slot QA liberi che ha visto transitare sul forward bus.

Questo algoritmo è ulteriormente complicato dalla presenza di tre livelli di priorità e quindi dalla necessità di gestire non una, ma tre code distribuite. Per analizzare più nel dettaglio il funzionamento dell'algoritmo supporremo per ora di avere una sola coda distribuita.

Le informazioni necessarie all'accesso sono contenute in due contatori:

- il *Request Count* (RQ);
- il *Countdown* (CD).

Esistono due coppie di contatori, per ogni priorità, in ogni Access Unit. Una coppia è utilizzata quando il forward bus è A, mentre l'altra quando il forward bus è B.

Il contatore RQ si incrementa ad ogni richiesta di accesso ricevuta sul reverse bus e si decrementa ad ogni slot QA libero che transita sul forward bus (figura 9.10).

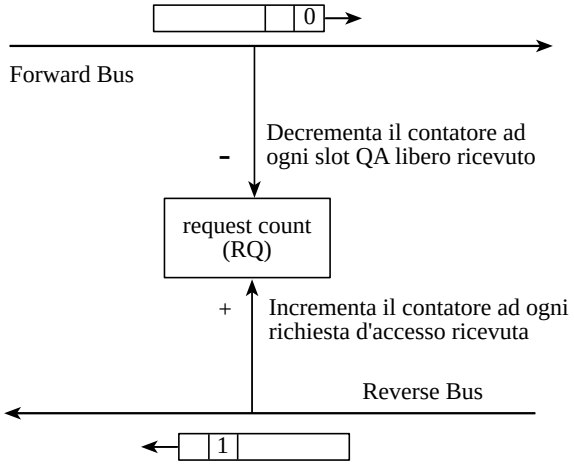


Fig. 9.10 - Nodo privo di segmenti da trasmettere.

Quando una Access Unit ha un segmento da trasferire esegue le seguenti operazioni:

- in funzione della localizzazione del nodo destinatario, determina quale bus è il forward bus e quale il reverse;
- mette il segmento da trasferire nella coda di accesso del forward bus;
- imposta una richiesta di accesso sul reverse bus;
- copia il valore corrente del contatore RQ nel contatore CD (figura 9.11);
- azzera il contatore RQ e ricomincia a contare le richieste di accesso successive;
- inizia a contare gli slot QA liberi che transitano sul forward bus ed al passaggio di ognuno di questi decrementa il contatore CD;
- quando il contatore CD arriva a zero il segmento può essere trasferito;
- al passaggio del primo slot QA imposta il bit di busy per indicare che lo slot è stato utilizzato e trasferisce il segmento che era in coda.

DQDB prevede tre livelli di priorità: 0, 1 e 2. Il livello 0 è il più basso e deve essere utilizzato per i segmenti di dati di tipo non connesso. Gli altri livelli di priorità sono riservati per usi futuri.

Per gestire tre code a priorità diversa nell'ACF (figura 9.8) sono presenti tre bit di richiesta e i contatori RQ e CD sono replicati per ogni livello di priorità. I contatori operano in modo simile a quanto descritto per il caso di priorità singola, con l'eccezione che occorre considerare anche le richieste di priorità superiore.

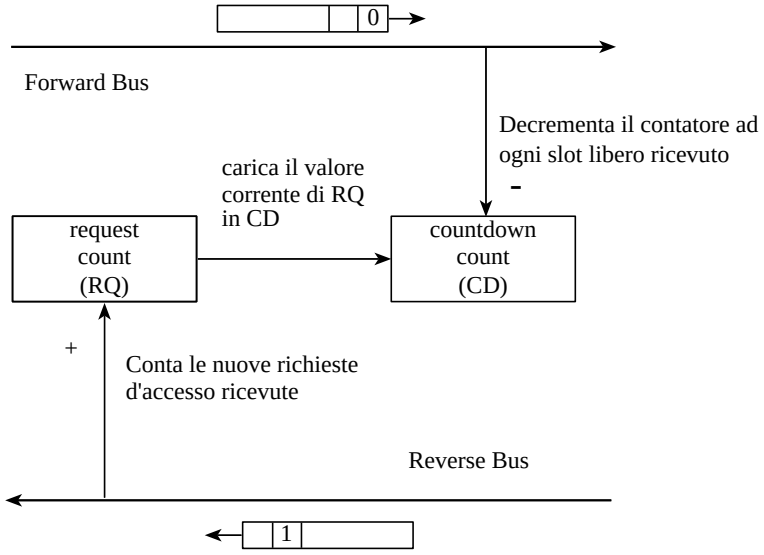


Fig. 9.11 - Nodo con segmenti da trasmettere.

Questo implica che quando uno slot in transito sul reverse bus contiene una richiesta di trasmissione ad una data priorità, occorre incrementare non solo il contatore RQ di quella priorità, ma anche i contatori RQ delle priorità inferiori.

Anche la gestione di CD è modificata, in quanto CD deve incrementarsi a fronte di una richiesta a priorità superiore sul reverse bus.

Occorre infine considerare che il transito di uno slot QA vuoto sul forward bus decrementa tutti i contatori RQ e CD.

9.2.5 Controllo d'accesso pre-arbitrato

Il controllo di accesso pre-arbitrato utilizza gli slot di tipo PA. Tali slot vengono generati dal nodo di head-of-bus che li marca di tipo PA.

Il segmento PA consiste in un insieme di ottetti, ognuno dei quali può essere usato da due o più Access Unit, cioè più Access Unit possono condividere l'accesso allo stesso slot.

Il nodo head-of-bus assegna lo slot ad un canale virtuale tramite la scrittura del campo VCI e assicura inoltre che per ogni canale virtuale sia disponibile una banda sufficiente per il servizio isocrono.

L'accesso ad uno slot PA da parte di una Access Unit inizia con l'osservazione del campo VCI. La Access Unit mantiene una tabella che indica, per ogni Virtual Channel, quali ottetti devono essere scritti o letti.

9.2.6 Servizi forniti dal MAC a LLC

Lo standard DQDB è stato progettato per fungere da dorsale di interconnessione di LAN diverse, quali IEEE 802.3, 802.4 e 802.5. DQDB è quindi in grado, in ambito urbano, di interconnettere tra loro più LAN installate in edifici non contigui.

A tal fine DQDB fornisce un servizio MAC non connesso al livello LLC sovrastante. Le MAC Service Data Unit (MSDU) vengono segmentate dal nodo DQDB mittente, i segmenti trasmessi sulla rete DQDB e ricevuti al nodo DQDB destinatario che li riassembla, ricostruendo le MSDU.

La componente logica di un nodo che ha il compito di operare la segmentazione e il riassemblaggio di un messaggio MAC si chiama MCF (MAC Convergence Function). Essa ha funzione di adattamento tra il formato dello slot DQDB ed i formati dei messaggi di altre LAN 802.x (figura 9.7).

Il trasferimento di una MSDU viene effettuato secondo le seguenti fasi (figura 9.12):

- creazione della IMPDU (*Initial MAC PDU*) che contiene nella parte INFO la MSDU da trasportare;
- segmentazione della IMPDU in parti lunghe 44 ottetti;
- aggiunta di uno header (2 ottetti) e di un trailer (2 ottetti) e formazione delle DMPDU (*Derived MAC PDU*), con lunghezza pari a 48 ottetti.

In funzione della lunghezza della IMPDU si possono porre tre casi:

- se la IMPDU ha una lunghezza inferiore o uguale a 44 ottetti si ha una singola DMPDU che è identificata con Segment Type uguale a SSM (*Single Segment Message*)*;*
- se la IMPDU ha una lunghezza inferiore o uguale a 88 ottetti si hanno due DMPDU di cui la prima ha Segment Type uguale a BOM (*Beginning Of Message*) e la seconda ha Segment Type uguale a EOM (*End Of Message*)*;*
- se la IMPDU ha una lunghezza superiore a 88 ottetti si hanno più DMPDU di cui la prima ha Segment Type uguale a BOM, quelle intermedie hanno segment type uguale a COM (*Continuation Of Message*), l'ultima ha segment type uguale a EOM.

Si noti che l'IMPDU header è totalmente contenuto nella prima DMPDU e cioè in una DMPDU SSM o BOM.

La figura 9.13 mostra il formato di una IMPDU. Si noti che i campi di destination address e source address sono di 8 ottetti, cioè 64 bit. Questa lunghezza consente di contenere sia gli indirizzi MAC che hanno lunghezza pari a 48 bit, sia gli indirizzi E.164 di derivazione telefonica (ISDN), con lunghezza pari a 60 bit.

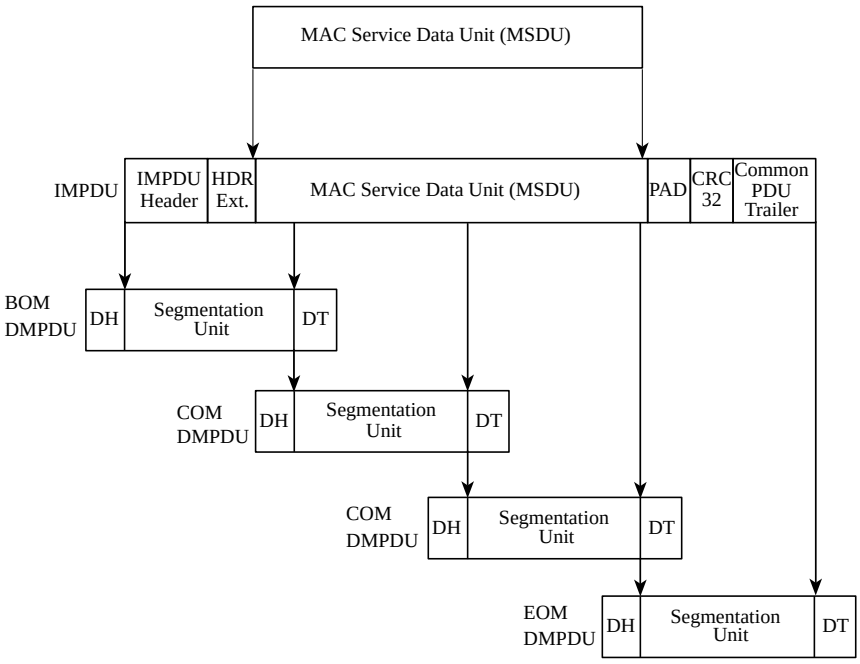


Fig. 9.12 - Segmentazione di una IMPDU.

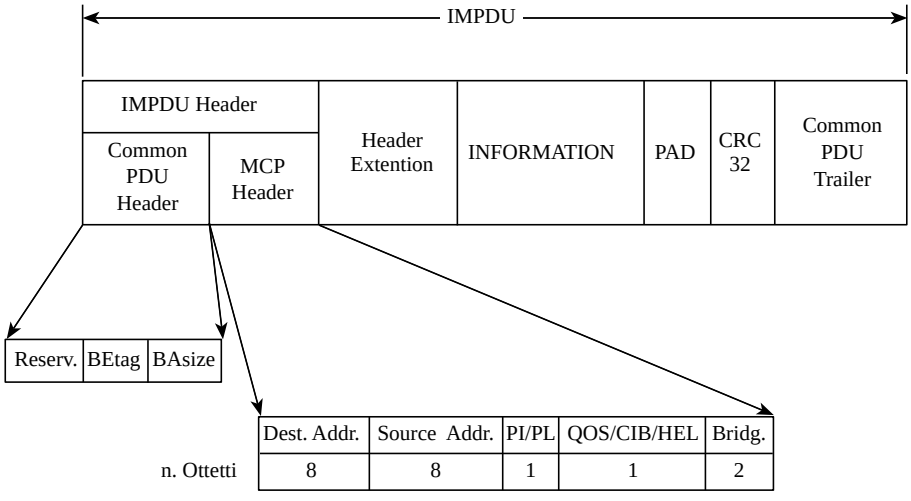


Fig. 9.13 - Formato di una IMPDU.

La figura 9.14 mostra il formato di una DMPDU. Si noti che la lunghezza di una DMPDU è pari a 48 ottetti, in modo da riempire totalmente il campo di segment payload (si veda figura 9.8).

In fase di ricezione una Access Unit verifica il campo VCI nell'header del segmento; per le MSDU contenenti una LLC-PDU il campo VCI contiene tutti uno. Se il valore di VCI è uno di quelli che la Access Unit è abilitata a ricevere si analizza il segment payload, cioè la DMPDU. Per prima cosa si verifica la payload CRC, se questa è errata il segmento viene scartato.

Per ogni DMPDU valida con Segment Type uguale a BOM si inizia un processo di riassemblaggio della IMPDU. Il riassemblaggio viene effettuato controllando il *sequence number* (le DMPDU hanno numeri crescenti modulo 16) e il MID (*Message IDentifier*) nell'header della DMPDU. Il MID contiene l'identificativo assegnato all'IMPDU in fase di segmentazione.

Sulla segmentazione e riassemblaggio di una MSDU vengono effettuati i seguenti controlli:

- lunghezza del messaggio, per evitare l'inserimento anomalo o la perdita di COM DMPDU;
- etichette BEtag (*Beginning-End tag*) delle BOM DMPDU e delle EOM DMPDU ricevute, per evitare di assemblare insieme due messaggi differenti;
- temporale (time-out), per verificare che l'EOM DMPDU arrivi entro un determinato tempo.

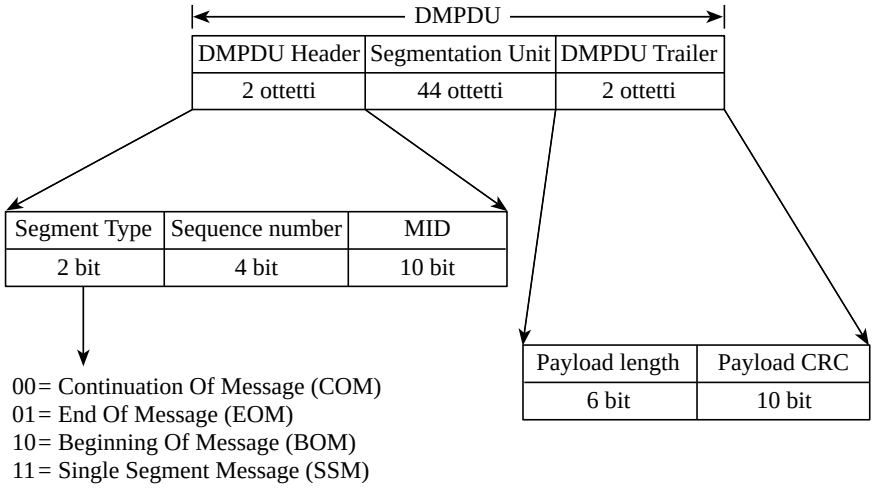


Fig. 9.14 - Formato di una DMPDU.

9.3 IL LIVELLO FISICO

La parte relativa al livello fisico dello standard IEEE 802.6 si occupa delle seguenti funzioni:

- interfacciamento con gli standard trasmissivi per le reti pubbliche;
- adattamento tra gli standard trasmissivi e il livello MAC, compito affidato alla funzione di PLCP (*Physical Layer Convergence Procedure*);
- controllo dello stato delle connessioni tramite la funzione di PLCSM (*Physical Layer Connection State Machine*).

Gli standard trasmissivi su rete pubblica attualmente previsti sono i seguenti:

- ANSI DS3 operante alla velocità di 44.736 Mb/s e definito nelle normative ANSI T1.102 e T1.107;
- CCITT G.703 operante alle velocità di 34.368 o 139.264 Mb/s;
- CCITT G.707, G.708 e G.709 SDH operante alla velocità di 155 Mb/s.

BIBLIOGRAFIA

[1] IEEE Std 802.6-1990, Distributed Queue Dual Bus (DQDB) Subnetwork of a Metropolitan Area Network (MAN).

[2] IEEE Std 802, "Overview and Architecture", IEEE, Piscataway N.J. (USA).

[3] ISO 8802-2 (ANSI/IEEE Std 802.2), "Logical Link Control".

10

INTERCONNESSIONE DI LAN TRAMITE BRIDGE

10.1 INTRODUZIONE

Le reti locali sinora esaminate hanno dei limiti in termini di distanze massime ammesse, carico massimo sopportato e numero massimo di sistemi collegabili. Quando si vuole oltrepassare uno o più di tali limiti, bisogna creare una *rete locale estesa* (a volte indicata con le sigle ELAN, XLAN o BLAN) interconnettendo tra loro più LAN per mezzo di *bridge*.

Nella figura 10.1 è rappresentato lo schema logico di una BLAN. I due sistemi* (End Station), connessi alle due LAN, sono messi in grado di comunicare dal bridge.

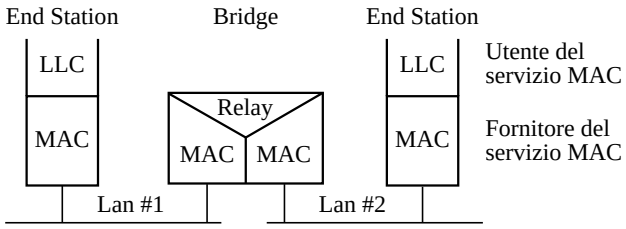


Fig. 10.1 - Impiego di un bridge per interconnettere due LAN.

I bridge ritrasmettono solo i pacchetti che devono effettivamente transitare da una LAN ad un'altra LAN, mantenendo separati i traffici locali delle singole LAN che interconnettono. Questa funzionalità, detta di "filtraggio" (*filtering*), permette

* Nel seguito il termine *sistema*, di derivazione OSI, e il termine *stazione* (station o end station), di derivazione IEEE 802, verranno usati come sinonimi.

di ottenere un traffico globale sulla BLAN superiore a quello massimo ammesso per ogni singola LAN.

Tale ritrasmissione avviene con una modalità di "*store and forward*", cioè il pacchetto è ricevuto dal bridge, e poi eventualmente ritrasmesso. Questo permette di superare i limiti sulle distanze massime e sul numero massimo di sistemi collegabili in una rete locale, in quanto tali limiti sono tipicamente dettati dal livello fisico.

I bridge possono interconnettere LAN con lo stesso MAC (es: 802.3 con 802.3) oppure con MAC differenti (es: FDDI con 802.3, FDDI con 802.5, 802.3 con 802.5). In questo secondo caso devono tradurre la busta di livello 2, ricevuta da una LAN, nella busta di livello 2 da trasmettere all'altra LAN. In figura 10.2 viene illustrato l'utilizzo di un bridge 802.3-FDDI e le relative operazioni di traduzione delle buste, che risultano semplici poiché entrambe le LAN utilizzano il protocollo IEEE 802.2/LLC (si veda paragrafo 5.7).

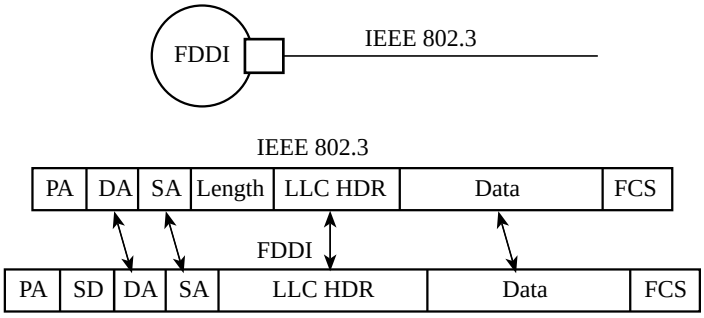


Fig. 10.2 - Bridge 802.3-FDDI.

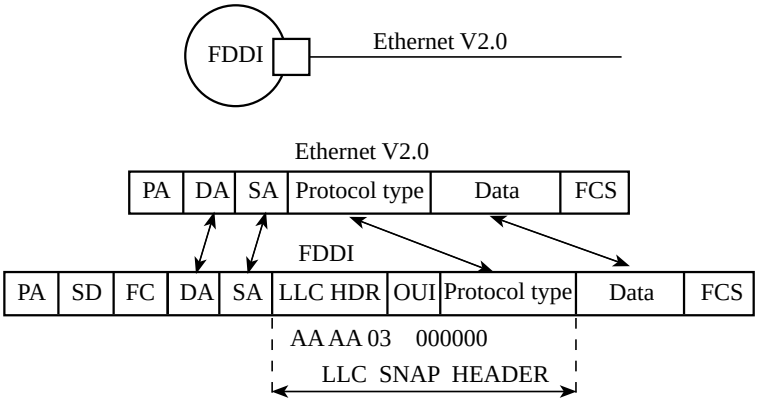


Fig. 10.3 - Bridge Ethernet-FDDI.

I bridge sono molto spesso utilizzati anche per interconnettere LAN proprietarie (non conformi allo standard IEEE 802). Il caso più tipico è quello dei bridge verso Ethernet. La figura 10.3 illustra un bridge Ethernet-FDDI e le relative problematiche di traduzione delle buste, che risultano più complesse poiché Ethernet non utilizza il protocollo IEEE 802.2 e il bridge deve inserire un header LLC SNAP (si veda il paragrafo 5.7.4).

10.1.1 Caratteristiche generali

I bridge hanno le seguenti caratteristiche generali:

- operano al livello 2 del modello di riferimento OSI, sottolivello MAC, e per questo sono molto spesso detti MAC-Bridge;
- hanno algoritmi di instradamento molto semplici: ogni bridge calcola autonomamente le sue tabelle di instradamento senza interagire con gli altri bridge, con un algoritmo di routing isolato (si veda il paragrafo 14.5.2);
- si utilizzano normalmente per interconnessioni locali, anche se sono stati usati nel passato, in modo un po' problematico, anche per interconnessioni geografiche.

I bridge possono essere realizzati secondo due filosofie diverse che differiscono nel luogo ove vengono memorizzate le *tabelle di instradamento* (nel seguito usato come sinonimo di *tabelle di filtraggio*):

- *transparent bridge*: sono i bridge conformi allo standard 802.1D (trattato in questo capitolo), di derivazione Ethernet. Hanno le tabelle di instradamento a bordo e sono trasparenti, nel senso che i sistemi interconnessi alle LAN ignorano la loro esistenza;
- *source routing bridge*: sono i bridge di derivazione token-ring. Non hanno tabelle di instradamento a bordo, le tabelle sono invece mantenute dai sistemi connessi alle LAN che in fase di trasmissione del pacchetto devono specificare esplicitamente il cammino che il pacchetto dovrà fare per giungere a destinazione, indicando tutti i bridge da attraversare (che quindi vengono indirizzati esplicitamente).

Nel seguito verranno descritti prima i transparent bridge e poi i source routing bridge. Quanto detto da questo punto in poi, quando non diversamente specificato, vale per i transparent bridge.

10.1.2 Spanning Tree

Come già visto, i bridge devono instradare pacchetti sulla rete e quindi hanno bisogno di costruirsi delle tabelle di instradamento. Se la topologia della BLAN è ad albero, la costruzione di tali tabelle può avvenire con un algoritmo molto semplice, in modo automatico, tramite un processo di apprendimento (*learning process*).

Poiché è tuttavia preferibile avere topologie magliate per ragioni di affidabilità, occorre integrare il learning process con un algoritmo di *spanning tree* (si veda paragrafo 10.18) per riportare dinamicamente una topologia magliata ad una topologia ad albero, escludendo dall'operatività opportune porte di opportuni bridge.

Tale problema non esiste nei source routing bridge, in quanto il pacchetto, quando viene generato, contiene la specifica completa del cammino che dovrà seguire.

10.1.3 Frammentazione

I bridge che operano tra LAN eterogenee hanno il problema aggiuntivo della diversa lunghezza massima del campo dati (INFO) del pacchetto MAC. La dimensione massima del campo INFO del pacchetto varia a seconda degli standard, ad esempio è di 1.500 byte per 802.3, 17.749 byte per 802.5 e 4.478 byte per FDDI.

Poiché è impossibile violare tali dimensioni massime, quando un bridge deve ritrasmettere un pacchetto di dimensione superiore a quella massima ammessa ha due possibilità: scartare il pacchetto o frammentarlo.

La frammentazione è un tipico compito del livello 3 (network) e non può essere realizzata da un bridge in modo generalizzato per tutti i protocolli. Fortunatamente molti di questi, tra cui ISO 8473 (si veda paragrafo 17.5) e DECnet fase IV (si veda paragrafo 15.2), non generano mai pacchetti più lunghi di 1500 byte e quindi il problema non si pone. Il protocollo TCP/IP invece genera sistematicamente pacchetti di dimensioni maggiori e molti bridge, limitatamente al protocollo IP (si veda paragrafo 16.4), realizzano la frammentazione, in accordo con lo standard RFC 791.

10.1.4 Prestazioni di un Bridge 802.3

Le prestazioni di un bridge sono importanti in quanto determinano le prestazioni globali della BLAN. I parametri più importanti sono:

- numero massimo di pacchetti al secondo che un bridge può filtrare (cioè ricevere e processare);

- numero massimo di pacchetti al secondo che un bridge può ritrasmettere;
- *tempo medio di latenza*, cioè tempo di attraversamento del bridge da parte di un pacchetto.

Per minimizzare la possibilità di perdita di pacchetti è preferibile che un bridge sia *full-speed*, cioè che i primi due parametri siano uguali al massimo teorico. Questo è tanto più difficile da realizzare quanto più i pacchetti sono corti (massimizza il numero di decisioni sul filtraggio che un bridge deve prendere nell'unità di tempo), per cui la proprietà di full-speed deve essere verificata con pacchetti tutti di lunghezza minima.

Nel caso di 802.3, un bridge è full-speed quando è in grado di inoltrare 14880 pps (packet per second) da 64 byte (pacchetti più corti). Tale numero si può calcolare partendo dalla lunghezza del pacchetto, aggiungendo preambolo e delimitatori e considerando la necessità di rispettare un *inter packet gap* tra i pacchetti, fissato da IEEE 802.3 in 9,6 microsecondi. La tabella 10.1 illustra le prestazioni di un bridge 802.3.

Dimensione pacchetto	Pacchetti al secondo	
	carico 50%	carico 100%
1.518	403	812
1.024	603	1.206
512	1.192	2.385
256	2.332	4.664
128	4.464	8.928
64	8.223	14.880

Tab. 10.1 - Prestazioni di un bridge 802.3-802.3.

Il tempo di latenza di un bridge esprime il tempo che intercorre da quando il pacchetto incomincia ad entrare nella porta ricevente a quando esso incomincia ad uscire dalla porta trasmittente. Il tempo di latenza non è fisso, ma varia a seconda della dimensione del pacchetto ricevuto: valori medi sono compresi tra 80 microsecondi e 1,2 millisecondi.

10.1.5 Bridge remoti

Nel progetto OSI i bridge sono stati concepiti per interconnettere LAN su base locale, mentre l'interconnessione di LAN su scala geografica è stata demandata ai

router, cioè a commutatori di pacchetto operanti al livello 3 del modello di riferimento OSI. Tuttavia, poiché i bridge sono assolutamente trasparenti ai protocolli di livello 3 (nel senso che trasportano qualsiasi pacchetto MAC valido, ignorandone il contenuto), e poiché si sono resi disponibili sul mercato prima dei router multi-protocollo, essi sono stati modificati per operare anche su scala geografica e sono nati i cosiddetti *bridge remoti.*

I bridge remoti vengono utilizzati per interconnettere le LAN anche geograficamente distanti e comunque implicano l'attraversamento di suolo pubblico. Essi utilizzano principalmente:

- linee telefoniche a velocità maggiore o uguale a 64 Kb/s;
- reti veloci a commutazione di pacchetto, quali Frame Relay e SMDS (si vedano i paragrafi 13.5 e 13.6);
- portanti non convenzionali, quali raggi laser, fibre ottiche e fasci di microonde.

Lo standard 802.1D non specifica le modalità ed i protocolli da usare per trasportare i pacchetti attraverso le linee pubbliche. Per questa ragione è consigliabile che la coppia di bridge remoti sia dello stesso costruttore e del medesimo modello. I protocolli più usati sulle linee sono HDLC e PPP (si vedano i paragrafi 13.2 e 13.3).

I bridge remoti non si prestano a realizzare strutture magliate, in quanto l'algoritmo di spanning tree mette in backup (stato di blocking) costose linee pubbliche sino a ridurre la rete ad un albero (figura 10.4), con evidente spreco di denaro.

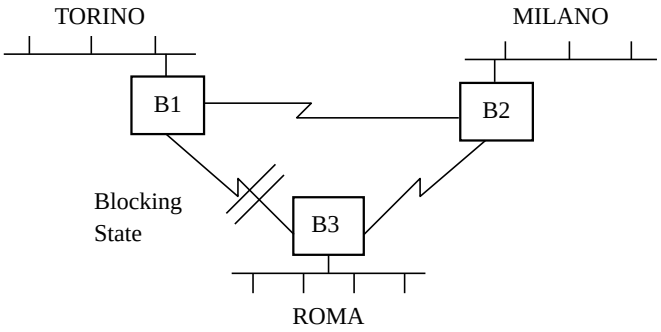


Fig. 10.4 - Bridge remoti

Alcuni costruttori, per utilizzare appieno tutte le linee, comprese quelle di backup, adottano il DLS (*Distribuited Load Sharing*). Il DLS permette di usare

anche le linee dichiarate in blocking state dallo spanning tree, per il traffico tra due LAN. I due problemi principali che devono essere risolti dal DLS sono il comportamento FIFO e la non generazione dei duplicati, e questo è particolarmente critico durante le fasi di transizione dello spanning tree.

10.2 ARCHITETTURA FISICA DI UN BRIDGE

I bridge sono costituiti da una o più CPU, una memoria e due o più interfacce che interconnettono le LAN (figura 10.5).

La ROM contiene il software che realizza tutte le funzionalità del bridge in conformità allo standard IEEE 802.1D. La memoria RAM contiene le tabelle di instradamento, i buffer per i dati ed un'area di memoria utilizzata dal software per le strutture dati interne.

L'interfaccia è costituita per una parte da dispositivi elettronici conformi ai diversi standard per le LAN (ad esempio, 802.3, 802.5, FDDI) e per la restante parte da dispositivi per la connessione ai diversi mezzi trasmissivi (ad esempio: UTP, STP, fibra ottica, cavo coassiale).

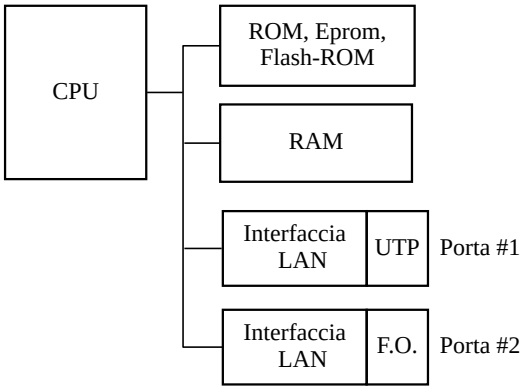


Fig. 10.5 - Architettura fisica di un bridge.

10.3 ARCHITETTURA LOGICA DI UN BRIDGE

Oltre a tale organizzazione fisica si può considerare un bridge costituito, da un punto di vista logico, dai seguenti tre elementi (figura 10.6):

- le *porte*, che possono essere due o più;
- l'entità di ritrasmissione e filtraggio chiamata *MAC relay entity*;
- le entità di livello superiore chiamate *higher layer entities*.

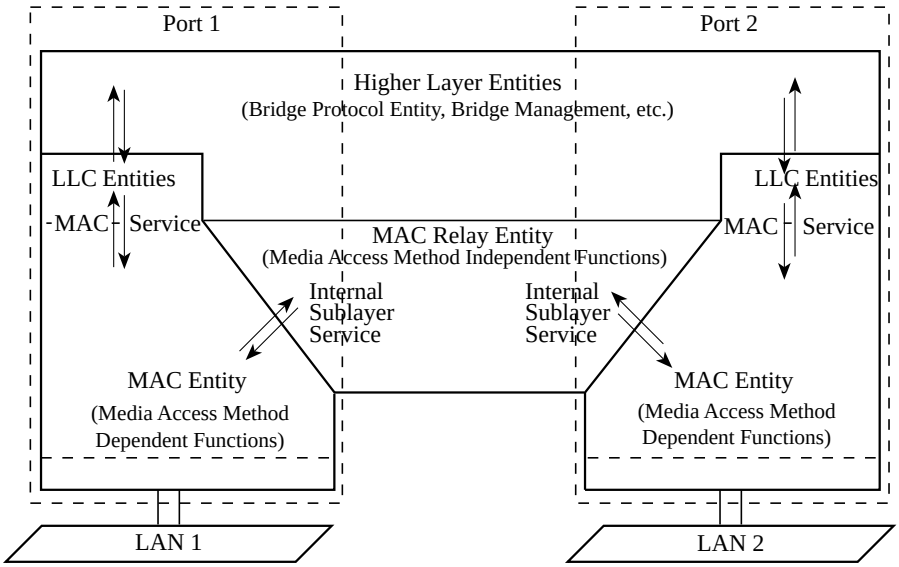


Fig. 10.6 - Architettura logica di un bridge.

Ogni porta riceve/trasmette i pacchetti dalla/alla LAN a cui è connessa usando il servizio fornito dall'entità MAC associata a tale porta. L'entità MAC di ogni porta tratta tutte le funzioni di metodo di accesso nel modo specificato dai relativi standard IEEE 802.

L'entità di ritrasmissione (MAC relay entity) si occupa di ritrasmettere i pacchetti tra due porte, filtrare i pacchetti ed apprendere le informazioni di filtraggio.

Le entità di livello superiore (higher layer entities), che fanno uso delle procedure di Logical Link Control (LLC), fornite separatamente per ogni porta, sono principalmente due:

- *bridge protocol entity* che si occupa del calcolo e della configurazione della topologia della BLAN (algoritmo di spanning-tree);
- *bridge management entity* che si occupa di governare e controllare le funzioni del bridge.

10.4 PRINCIPALI FUNZIONI DI UN BRIDGE

Le funzioni principali di un bridge sono:

- ricevere, filtrare e ritrasmettere i pacchetti;
- mantenere le informazioni richieste per prendere le decisioni di filtraggio;
- governare e controllare (*management*) quanto sopra citato.

La figura 10.7 riporta il diagramma di flusso relativo alle prime due funzioni.

10.4.1 Filtraggio

I pacchetti trasmessi da un sistema S1 verso un sistema S2 vengono confinati dai bridge nelle LAN che formano il percorso tra S1 e S2. Questo tipo di filtraggio è il più comune e serve a ridurre il traffico globale.

Qualora esistano più percorsi per raggiungere S2, i bridge operano un ulteriore filtraggio per prevenire la duplicazione di pacchetti.

Altri tipi di filtraggio possono essere effettuati intervenendo direttamente sul bridge con sistemi di management e definendo filtri inclusivi e filtri esclusivi. I filtri esclusivi limitano l'apprendimento del learning process, imponendo classi di pacchetti che devono essere sempre filtrati, cioè non ritrasmessi. I filtri inclusivi includono invece classi di pacchetti che non devono essere filtrati. Tali filtri possono agire su combinazioni dei seguenti parametri:

- indirizzo di mittente (MAC-SSAP) del pacchetto;
- indirizzo di destinatario (MAC-DSAP) del pacchetto;
- filtri basati sul tipo di protocollo di livello 3 contenuto nel campo dati della MAC-PDU.

Le funzioni che riguardano il mantenimento delle informazioni di filtraggio sono le seguenti:

- configurazione delle informazioni relative al filtraggio statico, cioè ai filtri inclusivi o esclusivi impostati da management;
- apprendimento automatico (learning process) delle informazioni relative al filtraggio dinamico, attraverso l'osservazione del traffico della BLAN;
- definizione dell'età massima (*ageing time*) delle informazioni di filtraggio che sono state apprese automaticamente, oltre la quale le informazioni stesse vengono invalidate;
- calcolo e configurazione della topologia della BLAN (tramite algoritmo di spanning-tree).

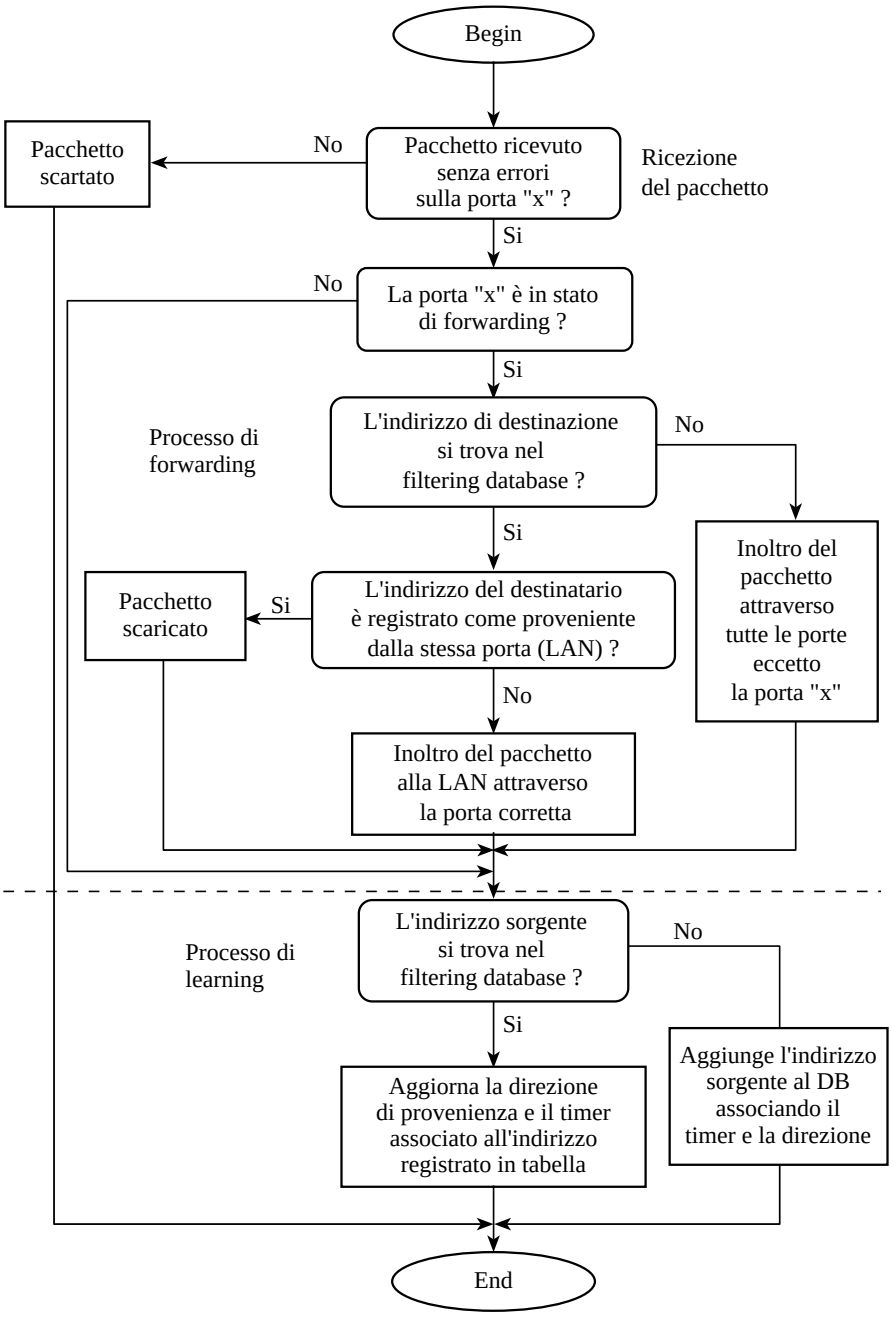

Begin
Pacchetto ricevuto senza errori sulla porta "x" ?
No
Pacchetto scartato
Ricezione del pacchetto
Si
La porta "x" è in stato di forwarding ?
No
Si
Processo di forwarding
L'indirizzo di destinazione si trova nel filtering database ?
No
Si
Inoltro del pacchetto attraverso tutte le porte eccetto la porta "x"
L'indirizzo del destinatario è registrato come proveniente dalla stessa porta (LAN) ?
Si
Pacchetto scaricato
No
Inoltro del pacchetto alla LAN attraverso la porta corretta
Processo di learning
L'indirizzo sorgente si trova nel filtering database ?
No
Si
Aggiunge l'indirizzo sorgente al DB associando il timer e la direzione
Aggiorna la direzione di provenienza e il timer associato all'indirizzo registrato in tabella
End

Fig. 10.7 - Diagramma di flusso delle principali operazioni del bridge.

10.4.2 Ritrasmissione (Relay)

I pacchetti che superano il filtraggio sono ritrasmessi sulla LAN di destinazione con il protocollo di livello MAC proprio di tale rete e mantenendo la sequenza con cui i pacchetti sono stati ricevuti.

10.5 INFORMAZIONE DI STATO DELLE PORTE

L'informazione di stato associata ad ogni porta del bridge governa la sua partecipazione alla BLAN. A livello di management si dichiara la porta attiva (*enabled*) o non attiva (*disabled*). Le porte attive possono trovarsi in vari sottostati in funzione delle decisioni prese dall'algoritmo di spanning tree. Una porta attiva si dice in un stato di *forwarding* se partecipa alla ritrasmissione di pacchetti, di *learning* se si limita ad apprendere, di *listening* se si limita ad ascoltare il traffico e di *blocking* se è stata definita come porta di backup dall'algoritmo di spanning tree (per una descrizione più dettagliata si veda il paragrafo 10.18.3).

10.6 TABELLA DI INSTRADAMENTO

La tabella di instradamento, detta anche tabella di filtraggio o filtering database, è costituita da un insieme di righe (*entry*), contenenti le informazioni di filtraggio che sono esplicitamente configurate tramite operazioni di management (*entry statiche*) oppure sono state registrate automaticamente dal processo di apprendimento (*entry dinamiche*).

La tabella di instradamento fornisce le informazioni al processo di inoltro, per decidere se inoltrare un pacchetto avente un certo indirizzo di destinazione su una data porta.

Una entry dinamica non viene creata se esiste già una entry statica relativa allo stesso indirizzo MAC. All'atto della creazione di una entry statica, una eventuale entry dinamica relativa allo stesso indirizzo MAC viene rimossa.

Le entry dinamiche sono soggette ad un meccanismo di timeout: se l'entry non viene aggiornata per un tempo superiore al parametro ageing time (valore di default cinque minuti), la entry viene automaticamente rimossa.

Le entry statiche non sono soggette a timeout.

10.7 RICEZIONE DEI PACCHETTI

L'entità MAC associata ad ogni porta riceve ed esamina tutti i pacchetti trasmessi sulla LAN cui è connessa.

La prima analisi riguarda il campo FCS per determinare se il pacchetto è corretto o errato. I pacchetti errati sono scartati.

I pacchetti indirizzati effettivamente alle entità di livello superiore del bridge (che sono normalmente una piccola parte) vengono affidati al livello LLC associato alla porta di ricezione. Questi pacchetti contengono nel campo destination (MAC-DSAP) l'indirizzo MAC di una porta del bridge o un indirizzo di gruppo (multicast) cui appartiene almeno una porta del bridge (ad esempio, l'indirizzo di multicast usato dal protocollo spanning tree).

Gli altri pacchetti vengono passati all'entità MAC di inoltro.

10.8 TRASMISSIONE DI PACCHETTI

L'entità MAC associata ad una porta trasmette i pacchetti che le sono stati affidati dall'entità MAC di inoltro dei pacchetti (MAC relay entity).

Essa trasmette inoltre i pacchetti generati dalle entità di livello superiore del bridge stesso.

10.9 INOLTRO DEI PACCHETTI

Il processo di inoltro dei pacchetti (frame forwarding) realizza la MAC relay entity e compie le seguenti funzioni:

- inoltro dei pacchetti ricevuti da una porta alle altre porte;
- filtraggio dei pacchetti in base alle informazioni contenute nella tabella di filtraggio;
- filtraggio dei pacchetti in base allo stato delle porte.

La figura 10.8 illustra l'utilizzo, da parte del processo di forwarding, dell'informazione di stato delle porte, allo scopo di determinare se il pacchetto debba essere ritrasmesso verso le altre porte del bridge.

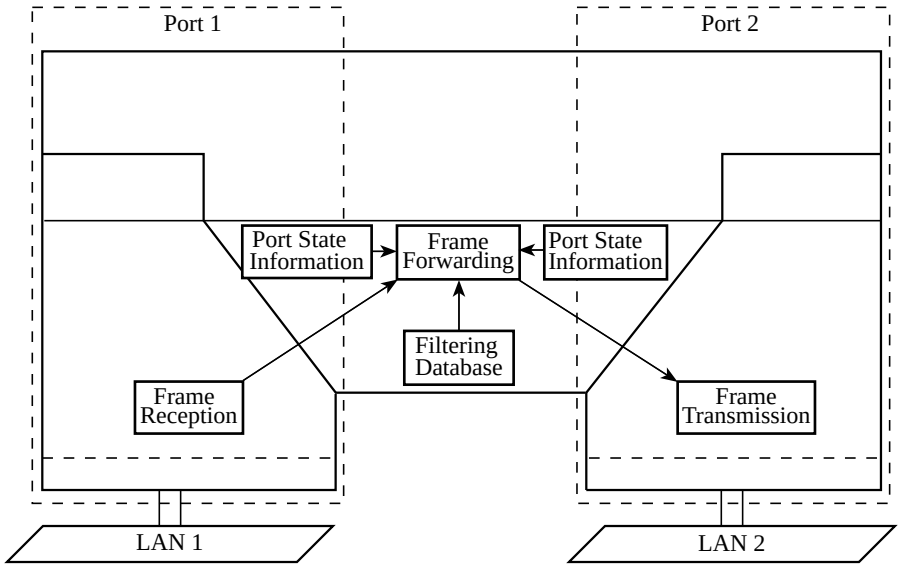


Fig. 10.8 - Inoltro dei pacchetti (bridge forwarding).

10.9.1 Condizioni di inoltro

Un pacchetto ricevuto su una porta di un bridge viene affidato al processo di inoltro che deve deciderne un eventuale accodamento per la trasmissione su altre porte. Condizione necessaria è che sia la porta di ricezione sia le porte di destinazione si trovino in stato di forwarding.

Il processo di inoltro accoda il pacchetto su una singola porta se questo ha un indirizzo di destinazione MAC (MAC-DSAP) di tipo singolo, su tutte le porte se il MAC-DSAP è multicast o broadcast.

Il processo di inoltro consulta la tabella di instradamento per determinare su quale porta eventualmente accodare il pacchetto in funzione del suo indirizzo di destinazione (MAC-DSAP).

È inoltre indispensabile che la dimensione del pacchetto da trasmettere non superi la dimensione massima ammessa dalla LAN di destinazione. Ad esempio, se il pacchetto ricevuto ha una dimensione di 2.052 byte ed è destinato ad una LAN 802.3, il pacchetto non verrà inoltrato, poiché la dimensione massima del campo dati nelle LAN 802.3 è di 1500 byte.

10.9.2 Accodamento dei pacchetti

Il processo di inoltro si occupa di accodare i pacchetti rispettando l'ordine di arrivo, operando cioè in modalità FIFO (*First-In First-Out*).

Un pacchetto viene rimosso dalla coda della porta a cui è associato a seguito di una delle seguenti condizioni:

- dopo la trasmissione del pacchetto stesso, indipendentemente dal fatto che sia avvenuta correttamente;
- nel caso in cui venga superato il tempo massimo di transito del pacchetto (*maximum bridge transit delay*);
- nel caso in cui la porta abbandoni lo stato di forwarding.

La rimozione di un pacchetto dalla coda di trasmissione di una porta non implica la rimozione del medesimo dalla coda di trasmissione di altre porte.

10.9.3 Ricalcolo della FCS

Quando un pacchetto viene inoltrato tra due LAN omogenee non viene effettuato il ricalcolo del FCS, qualora invece le due LAN siano eterogenee (ad esempio, un pacchetto ricevuto su una porta associata ad una LAN IEEE 802.3 e ritrasmesso ad una LAN FDDI) viene ricalcolato il campo FCS.

10.10 PROCESSO DI APPRENDIMENTO

Il processo di apprendimento (learning) osserva l'indirizzo MAC sorgente (MAC-SSAP) dei pacchetti ricevuti su ogni porta e crea o aggiorna le entry dinamiche della tabella di instradamento, condizionatamente allo stato delle porte.

Il MAC-SSAP indica al processo di apprendimento che la stazione con quell'indirizzo è raggiungibile attraverso la porta che ha ricevuto il pacchetto. Tale metodologia di apprendimento è anche detta di *routing isolato - backward learning* (si veda il paragrafo 14.5.2) in quanto un indirizzo di sorgente attuale crea o aggiorna una entry dinamica della tabella di instradamento relativamente ad una destinazione che potrà essere utilizzata in futuro.

La figura 10.9 illustra il ruolo dell'informazione di stato relativa alla porta che riceve il pacchetto, allo scopo di determinare se l'informazione relativa alla locazione della stazione possa essere incorporata nel filtering database. In caso

positivo, nella tabella di instradamento viene inserito l'indirizzo MAC della stazione trasmittente e la direzione, cioè la porta del bridge da cui è stato ricevuto il pacchetto.

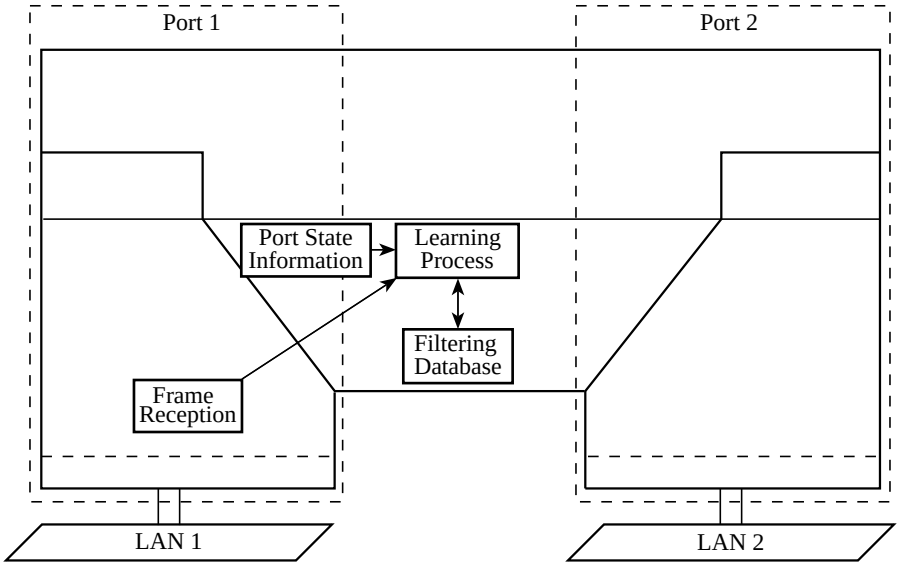


Fig. 10.9 - Processo di apprendimento.

Le condizioni in cui è possibile creare o aggiornare una entry dinamica sono:

- la porta da cui è stato ricevuto il pacchetto deve essere in uno stato che permetta l'apprendimento dell'indirizzo MAC (stato di learning o di forwarding);
- non esiste già una entry statica per quell'indirizzo MAC.

Se il numero risultante di tutte le entry supera la capacità massima della tabella di instradamento, una entry più vecchia viene rimossa per far spazio alla nuova entry.

10.11 BRIDGE MANAGEMENT

Lo standard IEEE 802.1B specifica i protocolli e le operazioni relative al management remoto dei bridge. I protocolli di bridge management fanno uso del servizio fornito dai sottolivelli LLC del bridge.

10.12 INDIRIZZAMENTO

Le entità MAC che comunicano attraverso una BLAN adottano il classico indirizzo MAC su 48 bit (si veda il paragrafo 5.6.7). In particolare, sia le porte dei bridge, sia i bridge stessi devono avere un indirizzo MAC. Gli indirizzi delle porte sono utilizzati dai protocolli di spanning tree e di management. Le porte vengono inoltre identificate all'interno del bridge con un numero progressivo a partire da 1. L'indirizzo del bridge coincide con l'indirizzo MAC della porta 1.

10.13 ENTITÀ DI PROTOCOLLO DEI BRIDGE

Le entità di protocollo dei bridge (*bridge protocol entities*) realizzano l'algoritmo di spanning tree. Esse operano tramite le BPDU (*Bridge Protocol Data Unit*) trasmesse in multicast all'indirizzo MAC denominato *bridge group address* (tabella 10.2).

Assignment	Value
Bridge group address	01-80-C2-00-00-00
Reserved for future standardization	01-80-C2-00-00-01÷ 01-80-C2-00-00-0F

Tab. 10.2 - Indirizzi di gruppo dei bridge.

Lo Standard 802.1D definisce inoltre il valore del LLC-SAP per il protocollo di spanning tree in 042H (in binario 01000010 è un numero palindromo e questo risolve alcuni problemi di incompatibilità tra gli standard relativamente a MSB e LSB).

La figura 10.10 illustra le operazioni effettuate dalle entità di protocollo dei bridge ed in particolare la modifica delle informazioni di stato delle porte e della tabella di instradamento. Tale modifica viene elaborata dall'algoritmo di spanning tree quando sia necessario determinare una nuova topologia attiva della BLAN.

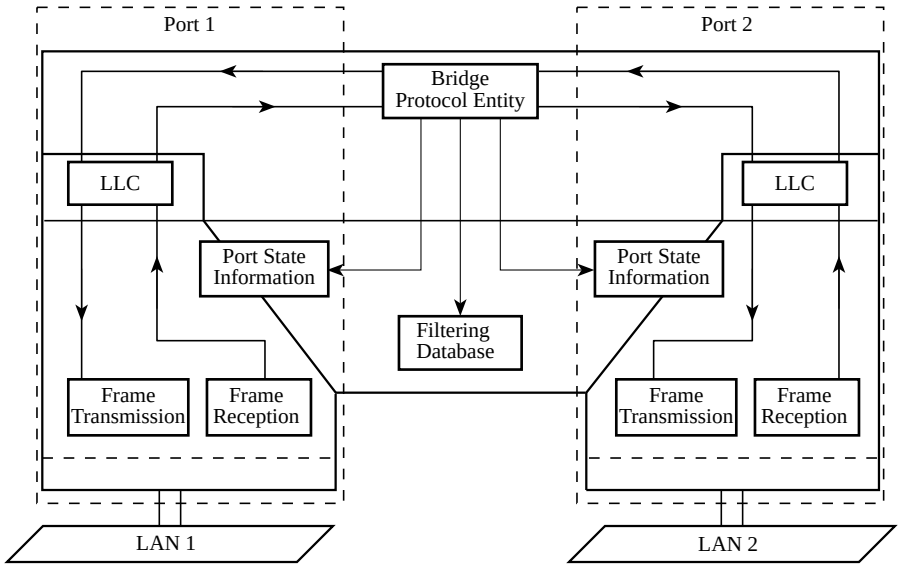


Fig. 10.10 - Entità di protocollo.

10.14 ENTITÀ DI MANAGEMENT DEI BRIDGE

Le entità di management dei bridge (*bridge management entities*) trasmettono e ricevono pacchetti di management, usando il servizio fornito dalle entità LLC associate alle porte. Lo standard IEEE 802.1D specifica l'indirizzo di multicast denominato *all LANs bridge management group address* (tabella 10.3). Tale indirizzo serve a raccogliere tutte le richieste delle entità di bridge management associate a tutte le porte dei bridge connesse alla BLAN.

Assignment	Value
All LANs bridge management group address	01-80-C2-00-00-10

Tab. 10.3 - Indirizzo riservato per il management dei bridge.

10.15 SUPPORTO DEL SERVIZIO MAC

I bridge realizzano le primitive MA_UNIDATA.request e MA_UNIDATA.indication di un servizio non connesso e non confermato (unacknowledged connectionless service).

Questo implica che quando un sistema trasmette un pacchetto indirizzato ad un altro sistema che si trova su un'altra LAN, il bridge non conferma alla stazione trasmittente l'avvenuta ritrasmissione del pacchetto. L'uso di servizi di tipo confermato non è ammesso.

Il servizio offerto da una BLAN è simile a quello di una singola LAN, di conseguenza un bridge non è direttamente indirizzato dai sistemi comunicanti, eccetto che per scopi di management del bridge stesso.

La presenza di bridge non deve porre restrizioni sulla posizione dei sistemi nella BLAN che deve poter variare dinamicamente (ad esempio, un PC portabile deve poter essere connesso prima a una LAN o poi ad una seconda LAN e i bridge devono adattare le loro tabelle di instradamento al cambiamento di posizione).

10.16 QUALITÀ DEL SERVIZIO

La qualità del servizio MAC offerto da una BLAN non deve essere significativamente inferiore a quella fornita da una singola LAN. I parametri da considerare in relazione alla qualità del servizio sono descritti nei seguenti sottoparagrafi.

10.16.1 Disponibilità del servizio

La disponibilità del servizio è misurata come la percentuale di tempo durante il quale il servizio è fornito. La presenza di un bridge può aumentare o ridurre la disponibilità del servizio.

La disponibilità del servizio può essere aumentata tramite la possibilità di riconfigurare automaticamente la BLAN, nel caso in cui uno dei percorsi non sia più disponibile a seguito di un guasto ad uno dei componenti (repeater, cavi, connettori).

La disponibilità del servizio può essere ridotta a seguito del guasto di un bridge o durante le operazioni di riconfigurazione della topologia di rete. Infatti, un bridge può bloccare il servizio e scartare i pacchetti, per preservare altri aspetti importanti del servizio MAC, quando avviene una riconfigurazione automatica, ad esempio per evitare la creazione di loop.

10.16.2 Pacchetti persi o fuori sequenza

Il servizio non connesso fornito dal sottolivello MAC non garantisce il recapito dei pacchetti. I pacchetti trasmessi dalla stazione sorgente hanno tuttavia

elevate probabilità di arrivare integri alla stazione destinataria. La presenza di un bridge incrementa leggermente la probabilità di perdita di pacchetti nei seguenti casi:

- il bridge non è in grado di trasmettere il pacchetto entro un certo tempo massimo *(maximum bridge transit delay)*, quindi deve scartarlo;
- il bridge non è in grado di immagazzinare altri pacchetti a causa della saturazione del buffer interno, in quanto i pacchetti continuano ad arrivare ad una velocità superiore a quella di inoltro;
- la dimensione del pacchetto eccede quella massima ammessa dal MAC della LAN di destinazione;
- durante un cambiamento di topologia il bridge deve scartare i pacchetti per un limitato periodo di tempo, in modo da garantire altri aspetti della qualità del servizio.

Il servizio fornito dai bridge garantisce una trasmissione ordinata dei pacchetti tra mittente e destinatario.

10.16.3 Duplicazione di pacchetti

I bridge non devono introdurre la duplicazione dei pacchetti. Questa, tuttavia, può essere causata da una trasmissione attraverso più bridge facenti parte di percorsi alternativi (figura 10.11). Questo potenziale problema viene risolto dall'algoritmo di spanning tree.

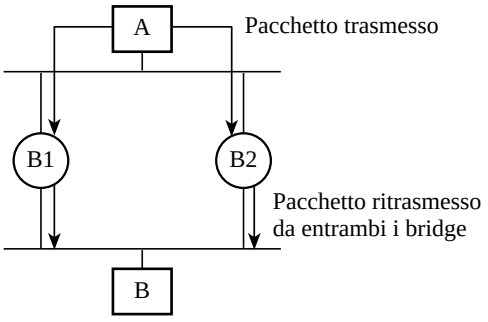


Fig. 10.11 - Duplicazione di pacchetti.

10.16.4 Ritardo di transito

Un bridge introduce un ritardo di transito addizionale poiché esso deve svolgere le seguenti funzioni prima di ritrasmettere il pacchetto ricevuto:

- aspettare di aver ricevuto completamente il pacchetto;
- verificare la FCS ed eventualmente scartare il pacchetto corrotto;
- controllare la tabella di instradamento per decidere se e dove inoltrare il pacchetto.

10.16.5 Dimensione massima della Service Data Unit

La dimensione massima della Service Data Unit (campo dati del pacchetto) ammessa da una LAN IEEE 802 varia in funzione del MAC e di altri parametri ad esso associati (ad esempio, la velocità).

La dimensione massima di pacchetto ammessa da un bridge che interconnette due LAN è quella inferiore ammessa dalle LAN. Ad esempio, se un bridge interconnette una LAN 802.3 e una LAN FDDI, userà come massima dimensione della Service Data Unit quella di 802.3 e cioè 1500 byte, invece di usare quella di FDDI che è di 4478 byte.

10.16.6 Throughput

Il throughput totale ammesso da una BLAN può essere significativamente maggiore di quello ammesso da una singola LAN. Ad esempio, il throughput globale della BLAN di figura 10.12 (cinque LAN 802.3, interconnesse da bridge full-speed) è di 50 Mb/s (10 Mb/s per 5 LAN).

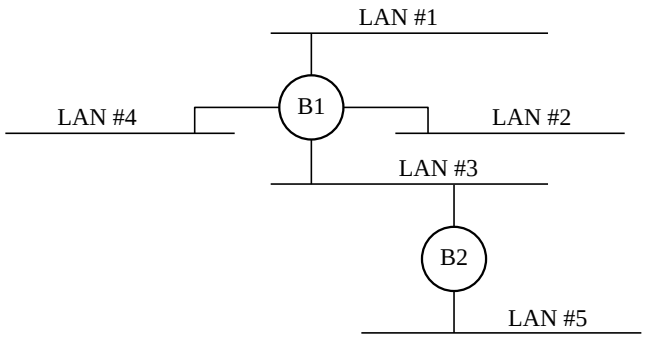


Fig. 10.12 - Throughput di una BLAN.

In figura 10.13 è riportato un esempio riferito ad una BLAN nella quale, a causa del bridge B che non è full-speed, e che ha quindi un inter frame spacing elevato, si ha una perdita di pacchetti quando la stazione A trasmette in continuazione pacchetti alla stazione E. In questo esempio, che rappresenta un caso limite, si ha una perdita del 50% dei pacchetti.

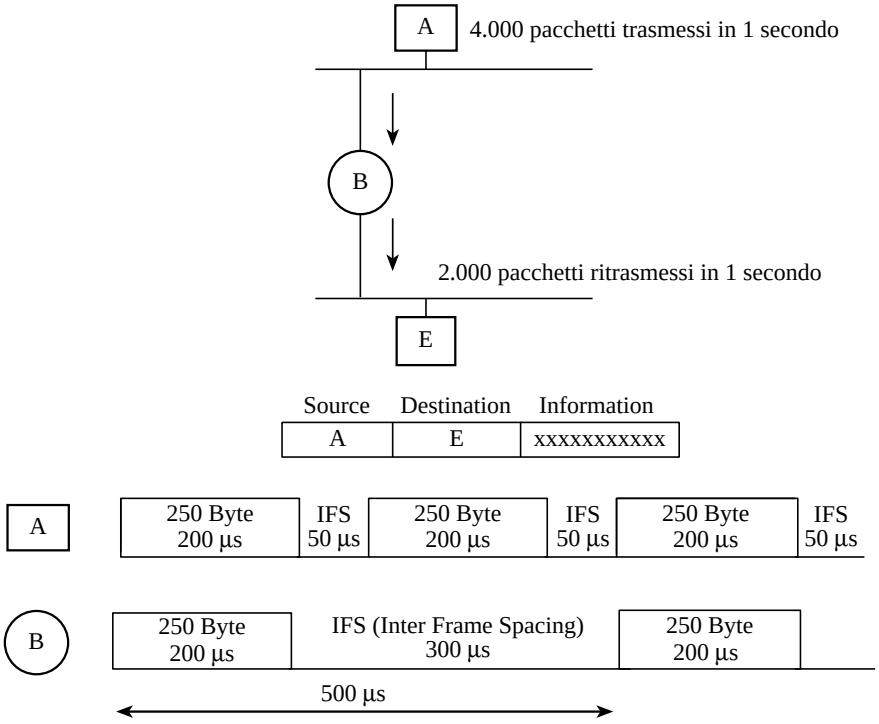


Fig. 10.13 - LAN interconnesse da bridge non full-speed.

10.17 SPANNING TREE

L'algoritmo di spanning tree riconfigura una topologia magliata di una BLAN in una topologia ad albero, eliminando i loop nel caso in cui ci siano più percorsi alternativi. In caso di guasto sul percorso primario, lo spanning tree deve riconfigurare automaticamente la topologia della BLAN, senza la formazione di loop nel transitorio. L'algoritmo di spanning tree opera attraverso un protocollo di spanning tree che genera BPDU (Bridge PDU).

Le caratteristiche desiderate dell'algoritmo di spanning tree sono:

- stabilizzare in breve tempo la topologia riconfigurata di una BLAN per ridurre il disservizio della rete;
- garantire che i percorsi tra sistemi siano prevedibili, riproducibili e configurabili tramite opportuni parametri;
- avere un limitato consumo di banda per le BPDU che i bridge si devono scambiare;
- ammettere che un bridge venga aggiunto alla BLAN senza che siano indispensabili operazioni di configurazione.

Per gestire la configurazione della topologia attiva l'algoritmo di spanning tree prevede l'assegnazione di una priorità ai bridge e alle porte di ciascun bridge. Tutti i bridge devono inoltre avere un identificatore univoco. A tal fine si definisce il *bridge ID* come la concatenazione della *priorità del bridge* definita da management (2 byte) e dell'indirizzo MAC del bridge (6 byte). Anche la *priorità della porta* (1 byte) è definita da management. I valori numerici più bassi indicano priorità maggiore.

La configurazione di una topologia attiva (albero) partendo da una topologia arbitraria (maglia) avviene ponendo alcune porte di alcuni bridge in blocking state. Infatti un bridge inoltra i pacchetti solo sulle porte che si trovano in forwarding state. Le porte che sono in blocking state non partecipano alla topologia attiva, ma sono pronte ad entrare a farne parte in caso di guasto di qualche componente della BLAN.

La figura 10.14 mostra un esempio di una BLAN configurata in modo magliato.

La figura 10.15 mostra una possibile topologia attiva della stessa BLAN.

10.17.1 L'algoritmo di spanning tree

L'algoritmo di spanning tree opera nei seguenti passi:

- *elezione del root bridge*: poiché si vuole identificare un albero, il primo passo consiste nell'identificare la radice dell'albero, cioè il *root bridge*. Il root bridge è per definizione il bridge che ha bridge ID minore;
- *selezione della root port*: per ogni bridge si identifica la porta più "conveniente" per interconnettere il bridge verso il root bridge. Tale porta è detta *root port*;

- *selezione del designated bridge:* per ogni LAN si sceglie quale bridge è designato a interconnettere la LAN con il root bridge. Questo passo è particolarmente importante quando esistono più cammini tra la LAN e il root bridge. Ogni LAN ha quindi un solo designated bridge che è il bridge "più vicino" al root bridge e che si incaricherà di trasmettere i pacchetti verso il root bridge. La porta del designated bridge che interconnette la LAN è detta *designated port*. Il root bridge è l'unico bridge che ha tutte designated port.

Al termine di questi tre passi si può procedere alla messa in stato di blocking delle porte che non sono né root né designated.

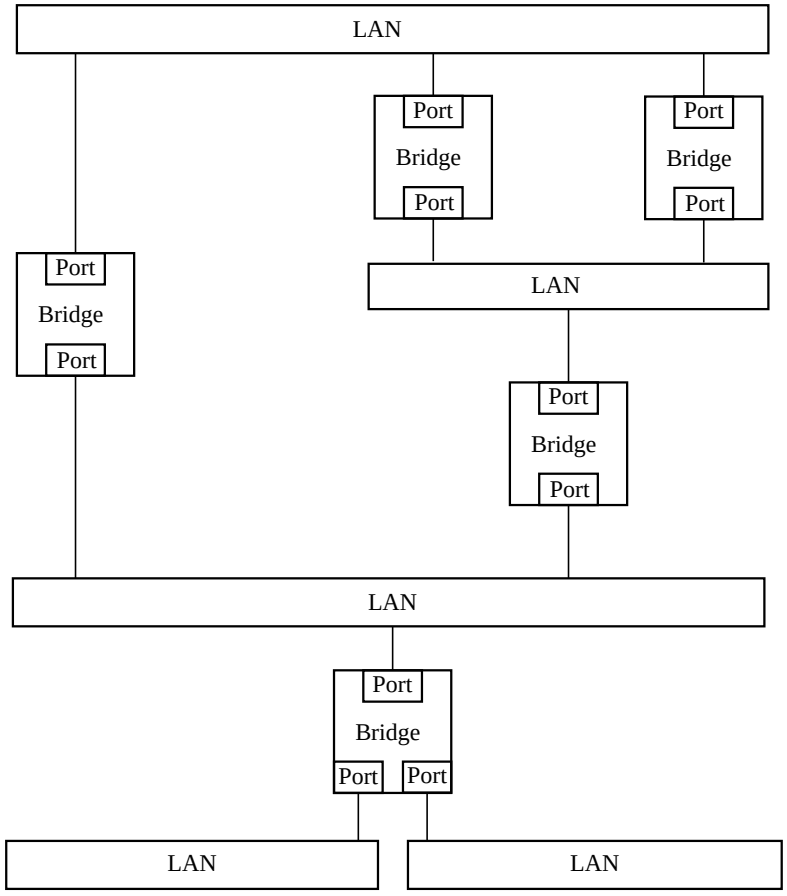


Fig. 10.14 - Una BLAN magliata.

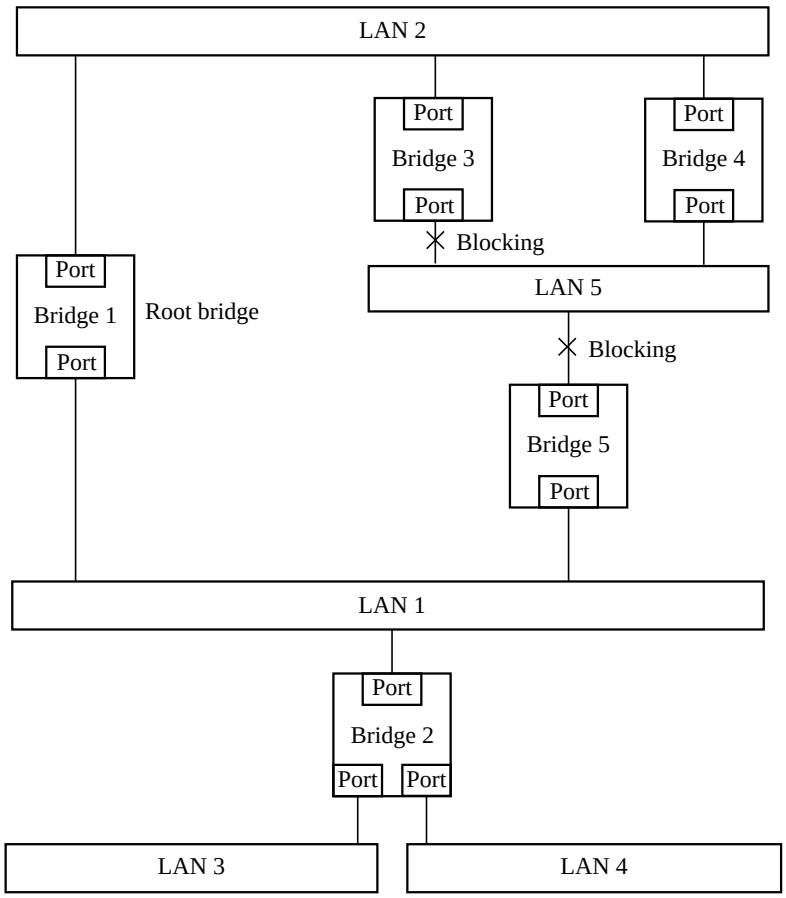


Fig. 10.15 - Topologia attiva ad albero.

In figura 10.15 il bridge 1 è stato eletto come root bridge ed è quindi il designated bridge per la LAN 1 e la LAN 2, il bridge 2 è il designated bridge per la LAN 3 e la LAN 4 e il bridge 4 è il designated bridge per la LAN 5. Le porte del bridge 3 e del bridge 5 collegate alla LAN 5 sono state messe in stato di blocking.

La figura 10.16 mostra lo spanning tree di questa configurazione attiva della BLAN.

Ogni porta ha un path cost che può essere configurato da management e che indica il costo di attraversamento di quella porta. Per ogni bridge e per ogni porta del bridge si definisce inoltre il *root path cost* come il costo totale di percorso per raggiungere il root bridge.

Il root path cost delle porte serve a due scopi:

- all'interno di un bridge, per scegliere quale sia la root port (quella che ha root path cost minore);
- tra le non root port dei bridge che si collegano su una LAN, per scegliere la designated port (quella che ha root path cost minore).

Il gestore della BLAN può controllare la formazione delle topologie attive intervenendo sui parametri bridge ID, port priority e path cost.

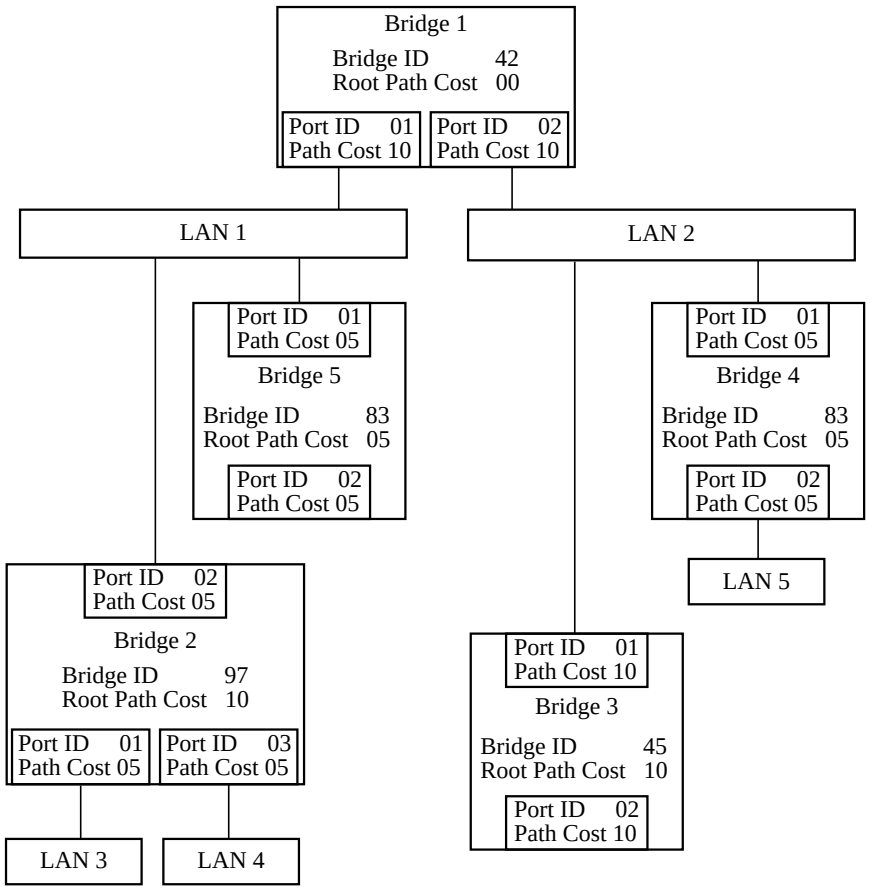


Fig. 10.16 - Esempio di spanning tree.

10.17.2 Bridge PDU e loro utilizzo nell'algoritmo di spanning tree

Le BPDU sono i pacchetti del protocollo 802.1D spanning tree che servono a realizzare il protocollo stesso.

Il root bridge genera periodicamente delle configuration BPDU (figura 10.17) che vengono trasmesse in multicast a tutti i bridge della BLAN. Gli altri bridge, quando ricevono una BPDU, ne aggiornano alcuni campi e la ritrasmettono sulle designated port.

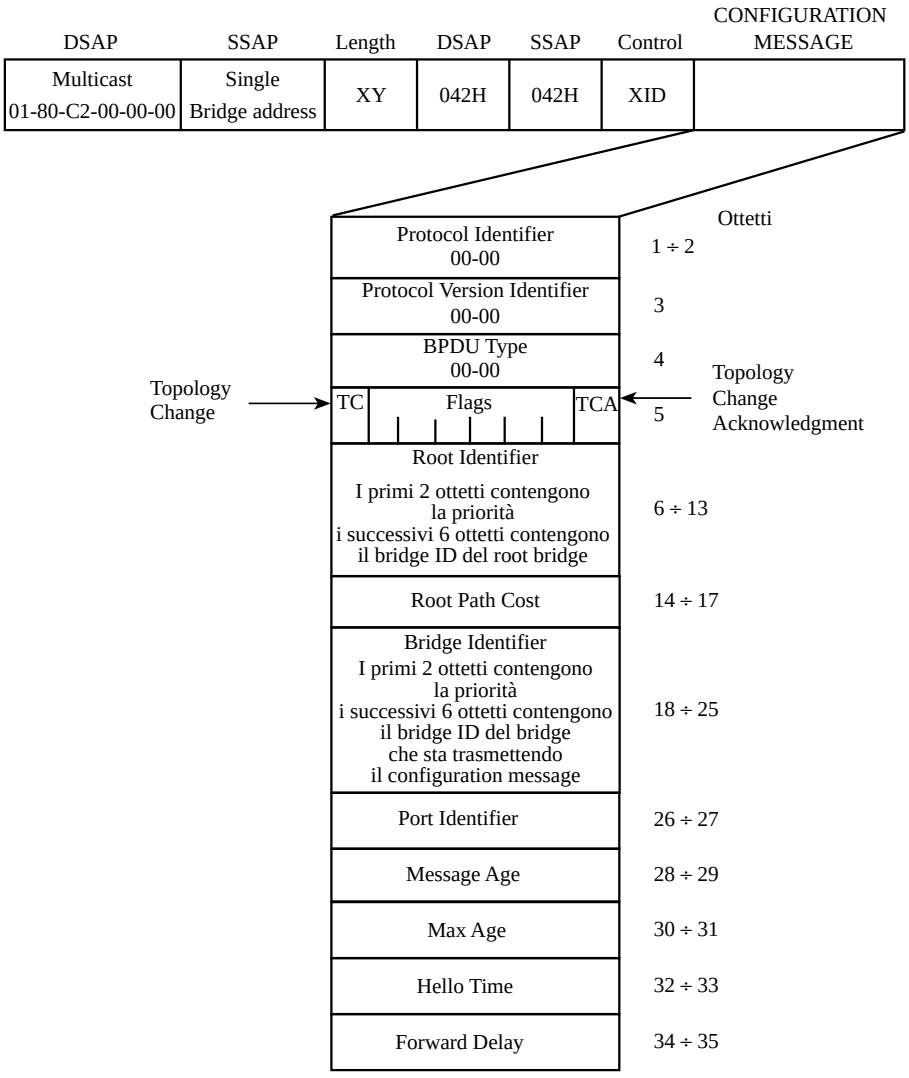


Fig. 10.17 - Configuration Bridge PDU.

I campi presenti in una configuration BPDU sono:

- *root identifier*: è l'identificatore del root bridge. Esso è composto da una prima parte di due ottetti, che è la priorità, e da una seconda parte di 6 ottetti, che è l'indirizzo MAC del root bridge;
- *root path cost*: è il costo totale di percorso per raggiungere il root bridge; questo valore è aggiornato ad ogni attraversamento di un bridge;
- *bridge identifier*: è l'identificatore del bridge che ha ritrasmesso il messaggio di configurazione. Esso è composto da una prima parte di due ottetti, che è la priorità, e da una seconda parte di 6 ottetti, che è l'indirizzo MAC del bridge;
- *port identifier:* è l'identificatore della porta da cui è stata trasmessa la BPDU. Esso è composto da una prima parte (primo ottetto) che è la priorità e da una seconda parte (secondo ottetto) che è il numero identificativo della porta (il valore zero non è ammesso);
- *message age*: è il tempo stimato (in multipli di 4 millisecondi) trascorso da quando il root bridge ha generato la configuration BPDU;
- *max age*: è il valore massimo di tempo (in multipli di 4 millisecondi) trascorso il quale la configuration BPDU deve essere scartata;
- *hello time*: è l'intervallo di tempo che intercorre tra la generazione di due configuration BPDU successive;
- *forward delay*: indica il tempo di permanenza nello stato di listening prima di passare allo stato di learning e nello stato di learning prima di passare a quello di forwarding;
- *Topology Change* (TC): è un flag che viene impostato dal root bridge in tutti i pacchetti di configuration BPDU trasmessi a seguito della ricezione di un pacchetto di topology change notification BPDU o del rilevamento di un cambiamento di topologia;
- *Topology Change Acknowledgment* (TCA): è un flag che viene messo a uno in una configuration BPDU dal designated bridge di una LAN, in risposta ad un pacchetto di topology change notification BPDU.

Per comprendere il ruolo delle configuration BPDU assumiamo di trovarci in un istante iniziale in cui tutti i bridge vengono accesi contemporaneamente. Si verificano i seguenti fatti:

- ogni bridge crede di essere il root bridge (fino a quando non ha un diverso riscontro) e origina le configuration BPDU su tutte le LAN ad esso connesse ad intervalli regolari specificando come root bridge il suo bridge ID e come root path cost zero;

- quando un bridge riceve da un altro bridge una configuration BPDU confronta il bridge ID del bridge che ha generato la PDU con il suo bridge ID: se è minore esso smette di considerarsi un root bridge e quindi di generare le configuration BPDU.

Questo porta rapidamente all'elezione del root bridge, che diventa l'unico bridge che genera le configuration BPDU. Eletto il root bridge si procede nel seguente modo:

- ogni bridge riceve le configuration BPDU da tutte le porte ed autonomamente decide che la sua root port sia quella con il minor valore di root path cost. Nel caso in cui due o più porte presentino un root path cost uguale, verranno presi in considerazione i parametri di bridge identifier della BPDU e port identifier per selezionare la root port;
- un bridge che riceva una configuration BPDU "minore" (cioè che, paragonata ai parametri associati alla porta ricevente quali root path cost, bridge identifier e port identifier, risulti prioritaria) su una porta che esso considera essere una designated port per la LAN a cui è connessa, smette di considerare tale porta designated e la pone in blocking state in quanto la BPDU "minore" evidenzia l'esistenza di un cammino più conveniente verso il root bridge;
- le root port e le designated port sono messe in stato di forwarding, le altre in stato di blocking.

10.17.3 Notifica del cambiamento di topologia

Un bridge, durante la sua normale operatività, può accorgersi che la topologia attiva è stata riconfigurata senza che questo diventi evidente a tutti gli altri bridge. Questo può causare delle inconsistenze nelle tabelle di instradamento dei bridge che sono estremamente pericolose in quanto possono generare loop.

I loop nei bridge sono particolarmente temuti in quanto nelle MAC-PDU non c'è un contatore (*hop count*) che consenta di scartare un pacchetto che continua a girare su di un loop ed inoltre tali pacchetti possono facilmente moltiplicarsi se ritrasmessi da più di un bridge collegato alla stessa LAN.

Per questo motivo, non appena un bridge verifica un cambiamento di topologia, lo comunica al root bridge trasmettendo una *topology notification change BPDU* (figura 10.18). Tale PDU viene trasmessa sulla root port e il bridge che la riceve la ritrasmette sulla sua root port sino a quando la PDU arriva al root bridge. Il root bridge comunica tale cambiamento ponendo a 1 il *Topology Change flag (TC)* nella

configuration BPDU (figura 10.17). Il pacchetto di topology notification change viene ritrasmesso più volte dal bridge che l'ha generato fino a quando questo non riceve una risposta di acquisizione dal designated bridge della LAN su cui il pacchetto è stato trasmesso.

La conferma di acknowledgment (TCA) è contenuta nella configuration BPDU (figura 10.17).

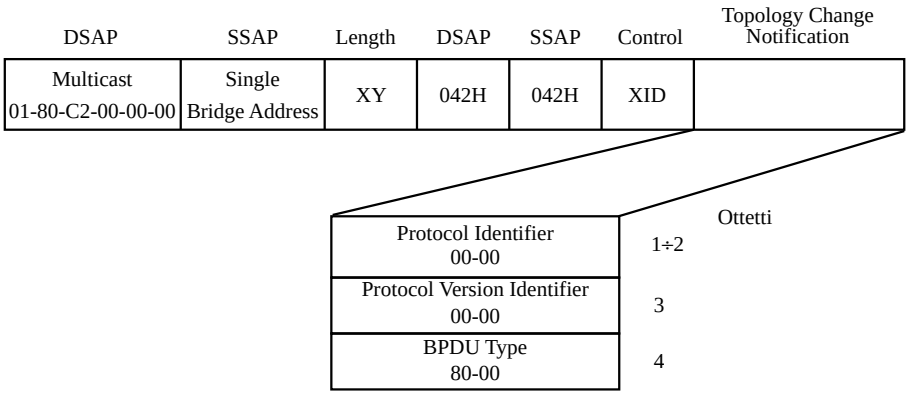


Fig. 10.18 - Topology Change Notification BPDU.

10.17.4 Cambio di stato delle porte

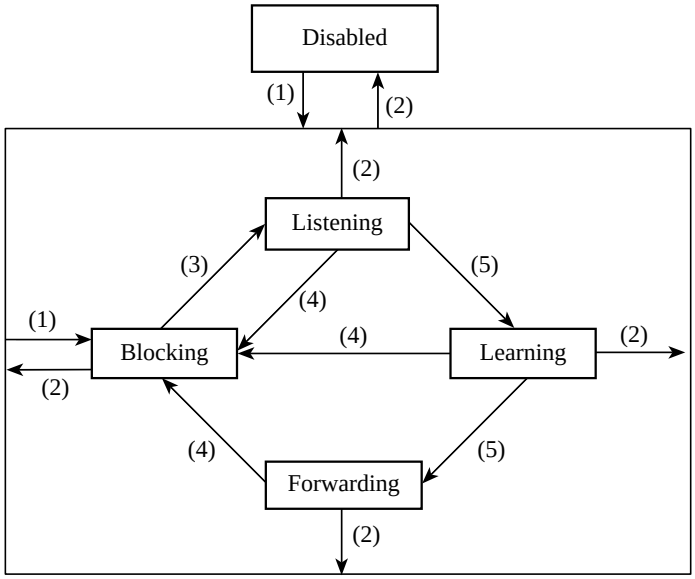
Il cambio di stato delle porte avviene seguendo precise sequenze, come viene rappresentato in figura 10.19. Esso può essere determinato sia dall'algoritmo di spanning tree, sia dal management.

Una porta *disabled* non partecipa alla topologia attiva della BLAN, mentre una porta *enabled* può partecipare alla topologia attiva della BLAN in funzione dello stato in cui si trova.

La transizione enabled-disabled e quella disabled-enabled sono controllate esclusivamente dal management o eventualmente in seguito all'insorgere di un guasto. Le porte enabled si possono trovare in uno degli stati sotto elencati.

- *Listening.* La porta si prepara a partecipare alla ritrasmissione dei pacchetti. Il processo di forwarding scarta tutti i pacchetti ricevuti. Il processo di learning non aggiunge nuove informazioni alla tabella di instradamento. La porta abbandona questo stato allo scadere del forward delay time per passare in stato di learning.

- *Learning*. La porta si prepara a partecipare alla ritrasmissione dei pacchetti. Il processo di forwarding scarta tutti i pacchetti ricevuti, ma il processo di learning aggiunge le informazioni ricevute alla tabella di instradamento. La porta abbandona questo stato allo scadere del forward delay time per passare in stato di forwarding.
- *Forwarding*. La porta partecipa alla ritrasmissione dei pacchetti. Il processo di forwarding può inoltrare i pacchetti ricevuti. Il processo di learning aggiunge le informazioni ricevute alla tabella di instradamento.
- *Blocking*. La porta non partecipa alla ritrasmissione dei pacchetti. Il processo di forwarding scarta tutti i pacchetti ricevuti. Una porta entra in stato di blocking perché ha ricevuto l'informazione che un'altra porta, facente parte del medesimo o di un altro bridge, è la designated port per la LAN a cui è connessa.



(1) Porta abilitata dal management o dall'inizializzazione
(2) Porta disabilitata dal management o da un guasto
(3) L'algoritmo seleziona la porta come una designated o root port
(4) L'algoritmo seleziona la porta come una "non designated port" o "non root port"
(5) Il forward delay timer è scaduto

Fig. 10.19 - Diagramma di stato delle porte.

10.17.5 Parametri raccomandati

Lo standard 802.1D raccomanda che non ci siano più di sette bridge in cascata e che vengano rispettati i parametri della tabelle 10.4, 10.5, 10.6 e 10.7.

Parameter	Recommended Value	Absolute Maximum
Maximum Bridge transit delay	1	4
Maximum BPDU transmission delay	1	4
Maximum Message Age increment overestimate	1	4

Tutti i tempi sono espressi in secondi

Tab. 10.4 - Ritardi di transito e trasmissione.

Parameter	Recommended or Default Value	Fixed Value	Range
Bridge Hello Time	2	-	1 ÷ 10
Bridge Max Age	20	-	6 ÷ 40
Bridge Forward Delay Timer	15	-	4 ÷ 30
Hold Time	-	1	-

Tutti i tempi sono espressi in secondi

Tab. 10.5 - Algoritmo di spanning tree - tempi consigliati.

Parameter	Recommended or Default Value	Range
Bridge Priority	32768	0 ÷ 65535
Port Priority	128	0 ÷ 255

Tab. 10.6 - Priorità dei bridge e delle porte - valori consigliati.

Parameter	Recommended Value	Absolute Minimum	Range
Path Cost	$\text{Path Cost} = \frac{1000}{\text{Attached LAN speed in Mb/s}}$	1	0 ÷ 65535

Tab. 10.7 - Parametro path cost - valore consigliato.

10.18 SOURCE ROUTING

Come già accennato nell'introduzione a questo capitolo, esistono anche dei bridge, progettati prima dello standard 802.1D, che usano una modalità detta *source routing*. Tali bridge sono stati concepiti per interconnettere esclusivamente LAN IEEE 802.5, e hanno avuto per un lungo periodo di tempo uno sviluppo parallelo a quello dei transparent bridge.

La necessità di interconnettere LAN 802.5 con LAN 802.3 fece nascere dei bridge denominati *source routing to transparent bridging* (SR-TB) che avrebbero dovuto risolvere il problema. Tali bridge risultarono molto complessi e si decise di abbandonarli.

Lo stato attuale degli standard prevede che i bridge standard siano transparent bridge e che la possibilità di effettuare source routing sia una prestazione addizionale. Un bridge in grado di realizzare source routing oltre al transparent bridging è detto *Source-Routing Transparent* (SRT) bridge.

Per semplicità di esposizione verranno illustrati prima i bridge puramente source routing e poi gli SRT.

10.19 BRIDGE PURAMENTE SOURCE ROUTING

I bridge source routing sono stati sviluppati per operare tra reti Token Ring in uno scenario simile a quello di figura 10.20. Essi sono esplicitamente indirizzati dalle stazioni che necessitano di inviare un messaggio sulla BLAN.

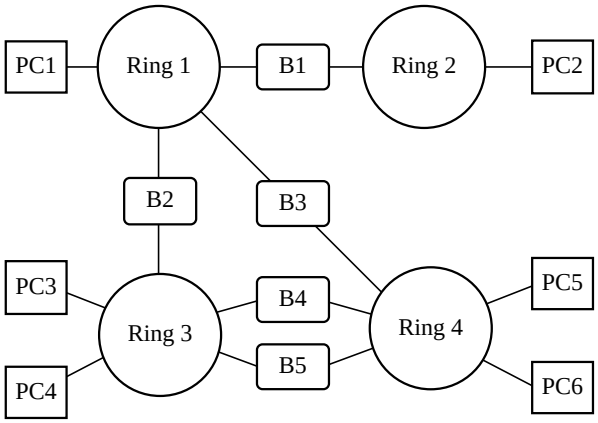


Fig. 10.20 - Una rete locale estesa Token Ring.

I bridge source routing basano l'instradamento del pacchetto sulle informazioni di percorso contenute nel pacchetto stesso nel campo RI (*Routing Information*). Quindi se PC1, in figura 10.20, vuole comunicare con PC6 deve specificare nel campo RI che intende far passare il pacchetto attraverso i bridge B2 e B5 oppure attraverso B2 e B4 oppure attraverso B3.

Se un pacchetto non ha un campo RI è un pacchetto destinato a un sistema connesso alla stessa LAN su cui è stato generato e viene quindi ignorato dai bridge.

I sistemi devono quindi mantenere a bordo una tabella di instradamento contenente le destinazioni con cui sono interessati a comunicare e che richiedono l'attraversamento di bridge. Le entry di tali tabelle vengono calcolate automaticamente tramite un processo chiamato *route discovery*. Questo processo permette al sistema mittente di scoprire dinamicamente il percorso per raggiungere il sistema destinatario utilizzando dei pacchetti di esplorazione della BLAN detti *All Routes Explorer (ARE) packet.*

Ogni bridge che inoltra un pacchetto multicast di route discovery ARE aggiunge al campo RI il suo identificativo e la massima dimensione ammissibile del pacchetto. In questo modo l'informazione d'instradamento viene costruita dai bridge al momento in cui il pacchetto di explorer viene inoltrato da un segmento di LAN ad un altro. Quando il pacchetto di explorer raggiunge la stazione di destinazione, esso contiene nel campo di RI tutte le informazioni di percorso e di massima dimensione del pacchetto ammissibile lungo l'intero percorso. La stazione di destinazione ritrasmette il pacchetto di explorer alla stazione mittente, che lo usa per calcolare la entry corrispondente nella tabella di instradamento. La stazione di destinazione riceve più copie del pacchetto di ARE, ma considera solo la prima in quanto ritenuta la più conveniente.

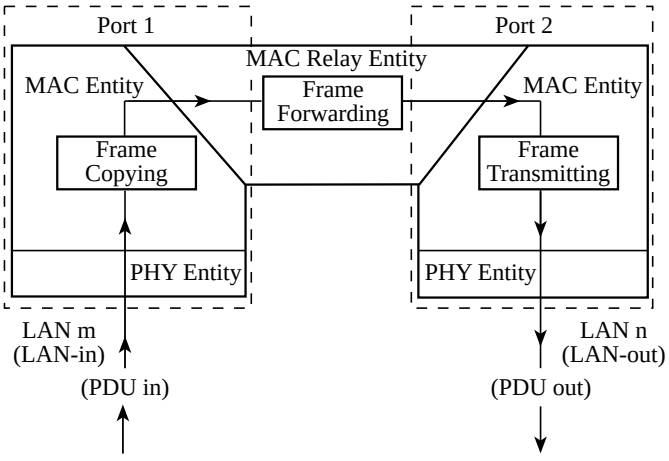


Fig. 10.21 - Elementi di un bridge source routing.

La figura 10.21 rappresenta gli elementi di un bridge source routing.

Poiché il campo RI non è presente in tutti i pacchetti token-ring, quando c'è è necessario indicarne la presenza. Per fare ciò, si utilizza il bit I/G (Individual/Global) dell'indirizzo MAC-SSAP (di mittente) che non serve non potendo valere altro che zero, essendo l'indirizzo di mittente sempre di un indirizzo singolo (figura 5.5). Tale bit viene ribattezzato RII e vale 0 in assenza di routing information e 1 in presenza di esse (figura 10.22).

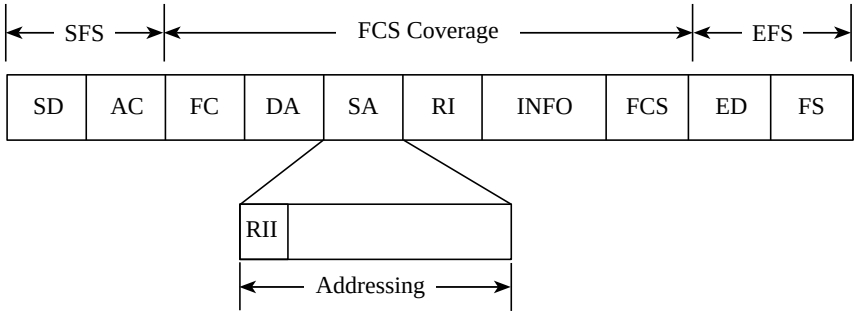


Fig. 10.22 - Formato del pacchetto 802.5.

10.20 SOURCE ROUTING TRANSPARENT BRIDGE

Un *Source-Routing Transparent (SRT) bridge* utilizza il metodo di source routing quando i pacchetti ricevuti contengono le informazioni di instradamento (RII = 1), ed utilizza il metodo transparent bridging quando i pacchetti ricevuti non contengono le informazioni di instradamento (RII = 0).

Il SRT bridge è l'unico bridge source routing riconosciuto a livello di standard.

Nella modalità source-routing esso opera nel seguente modo:

- il sistema mittente determina a priori l'instradamento del messaggio includendolo in ogni pacchetto;
- l'instradamento è espresso come una serie di identificatori (anello, bridge);
- i bridge non hanno tabelle di instradamento in quanto queste sono mantenute ed utilizzate dai sistemi mittenti;
- quando un sistema vuole imparare l'instradamento verso un altro sistema, invia un pacchetto di route explorer a cui il destinatario risponde;
- il meccanismo ammette fino a otto bridge in cascata.

Nella modalità transparent bridging, un SRT bridge opera esattamente come descritto nei precedenti paragrafi sui transparent bridge e quindi utilizza una tabella di instradamento locale, costruita come spiegato nel paragrafo 10.6.

Quindi per ogni pacchetto la decisione di inoltro è presa in base all'osservazione del campo RII dell'indirizzo MAC-SSAP: se è a 1, si utilizza l'informazione di instradamento contenuta nel campo RI, altrimenti la decisione di inoltro viene presa in base alla tabella di instradamento locale al bridge e all'indirizzo di destinazione (secondo la logica del transparent bridging). La figura 10.23 illustra l'architettura logica di un bridge SRT.

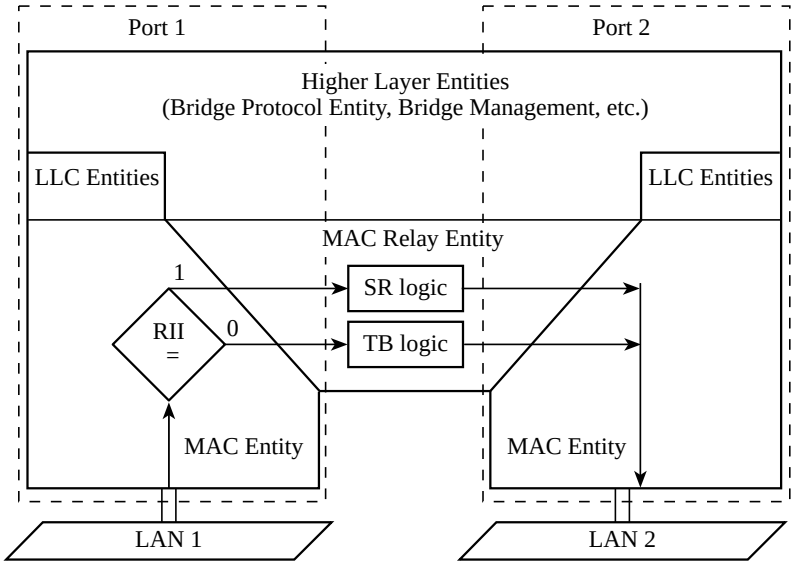


Fig. 10.23 - Schema logico di un bridge SRT.

10.20.1 Campo RI

Il campo di routing information è composto da due parti: il campo *routing control* (2 ottetti) e i campi *route descriptor* (da 2 ottetti ciascuno). La figura 10.24 illustra l'organizzazione del campo routing information.

I route descriptor contenuti nel campo RI possono essere al massimo 14 e quindi la lunghezza massima del campo RI è di 30 byte. La figura 10.25 illustra con maggiore dettaglio il campo routing information.

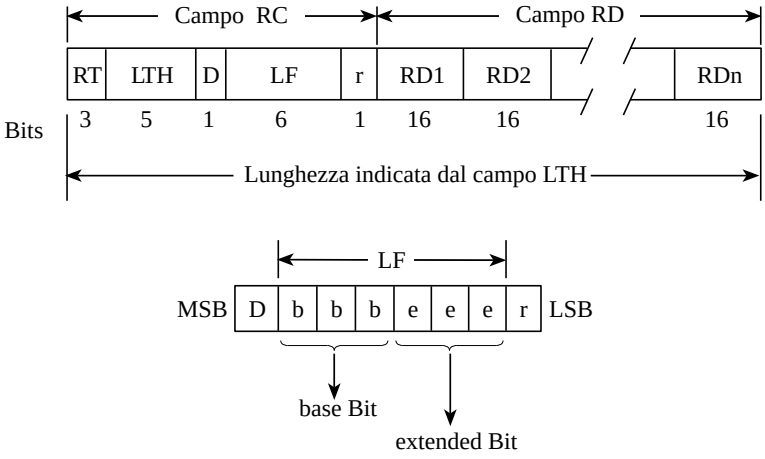


Fig. 10.24 - Campo RI.

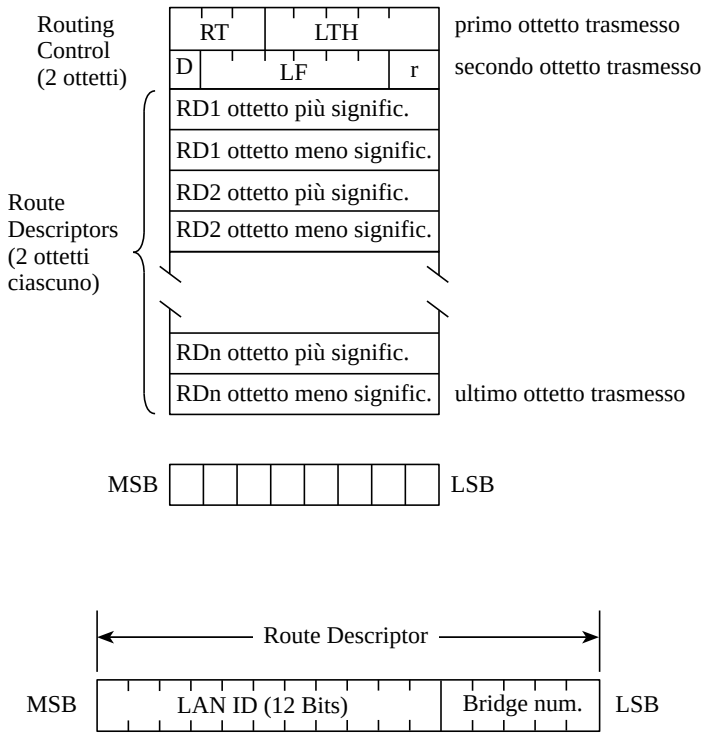


Fig. 10.25 - Dettaglio del campo RI.

10.20.2 Campo Routing Type (RT)

Questo campo indica se il pacchetto deve essere inoltrato attraverso la rete lungo un singolo percorso o lungo percorsi multipli. I routing type ammessi sono i seguenti:

- SRF *(Specifically Routed Frame)* (RT = 0XX). In questo tipo di pacchetto i campi RD (Route Descriptors) indicano un percorso specifico attraverso la rete;
- ARE *(All Routes Explorer frame)* (RT = 10X). Questo tipo di pacchetto viene instradato lungo tutti i percorsi della rete. Esso è originato da un sistema senza i route designators, che vengono aggiunti al pacchetto dai bridge SRT durante la fase di inoltro del pacchetto. Il sistema destinatario riceverà più pacchetti ARE i quali proporranno percorsi diversi;
- STE *(Spanning Tree Explorer frame)* (RT = 11X). Questo tipo di pacchetto può essere ritrasmesso da una LAN ad un'altra, solamente da una porta in *transparent bridging forwarding state*, con il risultato che il pacchetto verrà inoltrato a tutte le LAN appartenenti alla BLAN seguendo lo spanning tree, e raggiungerà ogni LAN una e una sola volta. L'utilizzo ovvio di questo tipo di pacchetto è per la trasmissione di pacchetti multicast.

10.20.3 Campo Length (LTH)

I cinque bit del campo indicano la lunghezza del campo RI in ottetti. La dimensione del campo RI è compresa tra due e trenta ottetti.

10.20.4 Campi LAN ID e bridge number

LAN ID è un identificativo univoco per ogni LAN assegnato dal gestore della BLAN. Poiché la tecnica SRT permette di avere percorsi multipli tra due LAN (tramite bridge collegati in parallelo), viene assegnato anche un numero di bridge (*bridge number*) ad ogni bridge. Tale bridge number non deve essere univoco su tutta la BLAN, ma solo nell'ambito dei bridge collegati in parallelo. Quindi un percorso tra due LAN è identificato da una serie di coppie {LAN ID, bridge number}.

10.20.5 Campo Direction (D)

Questo campo indica la direzione in cui il pacchetto attraversa la rete. Essa è indicata dal valore del bit D:

- se il bit D = 0, la direzione sarà quella specificata nel campo di Routing Information (da RD1 a RD2 ... a RDn);
- se il bit D = 1, la direzione sarà inversa a quella specificata dal campo di Routing Information (da RDn a ... RD2 a RD1).

Nei pacchetti STE e ARE il bit D è impostato a zero.

10.20.6 Campo di Largest Frame (LF)

I bit del campo indicano la dimensione massima del MAC Service Data Unit (parte INFO del pacchetto) che può essere trasmessa tra due stazioni comunicanti su uno specifico percorso (route). I bit del campo LF hanno significato solo per i pacchetti STE e ARE, mentre essi vengono ignorati dai pacchetti SRF. Una stazione che origina un pacchetto di explorer imposta i bit del LF alla massima dimensione che può trattare, i bridge che inoltrano il pacchetto potranno ridurre il valore contenuto in LF che non dovrà eccedere:

- il valore indicato dai bit LF ricevuti;
- la dimensione massima della MAC SDU ammessa dal bridge;
- la dimensione massima della MAC SDU ammessa dalla porta ricevente;
- la dimensione massima della MAC SDU ammessa dalla porta trasmittente.

La figura 10.24 illustra il campo LF e le tabelle 10.8, 10.9 e 10.10 illustrano i valori massimi di LF impostabili.

000:	516	ottetti (ISO 8473 più LLC)
001:	1.470	ottetti (ISO/IEC 8802.3, CSMA/CD)
010:	2.052	ottetti (matrice caratteri dello schermo 80x24)
011:	4.399	ottetti (ISO/IEC 8802.5, FDDI, 4 Mb/s Token Ring, ISO 9314-3)
100:	8.130	ottetti (ISO/IEC 8802.4 Token Bus)
101:	11.407	ottetti (ISO/IEC 8802.5 4-bit burst error unprotected)
110:	17.749	ottetti (ISO/IEC 8802.5 16 Mb/s Token Ring)
111:	41.600	ottetti (base per estendere fino a 65.535 ottetti)

Tab. 10.8 - Origine dei valori LF.

Base	Valore in ottetti	Base	Valore in ottetti
000	516	100	8.130
001	1.470	101	11.407
010	2.052	110	17.749
011	4.399	111	>17.749

Tab. 10.9 - Valori di Largest Frame base.

	EXTENSION								
BASE		000	001	010	011	100	101	110	111
	000	516	635	754	873	993	1.112	1.231	1.350
	001	1.470	1.542	1.615	1.688	1.761	1.833	1.906	1.979
	010	2.052	2.345	2.638	2.932	3.225	3.518	3.812	4.105
	011	4.399	4.865	5.331	5.798	6.264	6.730	7.197	7.663
	100	8.130	8.539	8.949	9.358	9.768	10.178	10.587	10.997
	101	11.407	12.199	12.992	13.785	14.578	15.370	16.163	16.956
	110	17.749	20.730	23.711	26.693	29.674	32.655	35.637	38.618
	111	41.600	44.591	47.583	50.575	53.567	56.559	59.551	>59.551

Tab. 10.10 - Valori di Largest Frame estesi.

BIBLIOGRAFIA

[1] Cisco Systems, "Internetworking Technology Overview", Codice documento DOC-ITO13 78-1070-01, 1993.

[2] R. Perlman, "Interconnections: Bridges and Routers", Addison Wesley, Reading MA (USA), 1992.

[3] Special Issue on Bridges, IEEE Network, Vol.2, No.1, January 1988.

[4] R.P. Davidson, N.J. Muller, "Internetworking LANs: Operation, Design and Management", Artech House, London (UK), 1992.

[5] IEEE Std 802, "Overview and Architecture", Piscataway N.J. (USA).

[6] ISO/IEC 10038 [ANSI/IEEE Std 802.1D] MAC Bridging, 1993.

[7] ISO/IEC 8802-5 [IEEE Std 802.5], "Token ring access method and physical layer specifications", 1992.

11

EVOLUZIONI DELLE LAN*

11.1 INTRODUZIONE

I costruttori di reti locali sono alla continua ricerca di soluzioni tecnologiche che consentano di ottenere reti locali più veloci, meno costose e più affidabili. Varie sono le proposte di evoluzioni, la più importante delle quali è senza dubbio l'adozione della tecnica ATM. Considerata l'importanza che avrà ATM nel futuro, non solo per le LAN, ma anche per le WAN, essa verrà trattata separatamente nei capitoli 19, 20 e 21. Tuttavia molte altre novità sono appena apparse sul mercato e le più significative verrano descritte in questo capitolo.

Gli sviluppi principali cui si sta assistendo hanno due obiettivi: migliorare le reti locali già esistenti, in particolare quelle di derivazione Ethernet, e creare reti locali wireless, cioè senza fili.

L'evoluzione verso il primo obiettivo ha portato alla disponibilità di una serie di prodotti che vengono presentati con vari nomi commerciali: Ethernet switch, Ethernet dedicato, Ethernet a 100 Mb/s (100BaseT e 100VG AnyLAN). Essi mirano a migliorare la più diffusa rete locale (Ethernet) fornendo a ciascun posto di lavoro 10 Mb/s dedicati oppure 100 Mb/s condivisi o dedicati.

La necessità di incrementare la velocità del singolo posto di lavoro è giustificata dalla crescente richiesta di applicazioni multimediali, le quali devono trasferire non solo dati, ma anche voce ed immagini; l'attenzione verso lo standard Ethernet è invece giustificata da considerazioni di mercato: si stima che nel

* Alla stesura di questo capitolo hanno dato un valido contribuito Marco Foschiano e Federico Micheletti, studenti del corso di Impianti di Elaborazione presso il Corso di Laurea in Ingegneria Informatica del Politecnico di Torino, ai quali vanno i più sentiti ringraziamenti degli autori per la preziosa collaborazione.

periodo 1984-1993 siano stati venduti 20.000.000 di nodi e che altrettanti ne saranno venduti nel periodo 1994-1996, dalle oltre 200 aziende produttrici.

Le reti wireless si pongono invece obiettivi diversi. Esse non sono nate con lo scopo di sostituire le reti cablate in quanto, almeno per ora, forniscono prestazioni nettamente inferiori, in alcuni casi anche di un ordine di grandezza, ma si pongono come un valido complemento ad esse fornendo all'utenza maggiore mobilità. Le reti di tipo wireless sono fortemente sinergiche con i calcolatori portatili tipo notebook e laptop in quanto consentono di veicolare i dati ovunque gli utenti si trovino: in ufficio, a casa o presso i clienti.

I fattori che spingono verso la realizzazione di reti locali wireless sono:

- la riduzione dei costi e delle dimensioni dei calcolatori portatili, unitamente all'incremento delle prestazioni, della capacità di memoria (centrale e di massa) e dell'autonomia;
- il desiderio, da parte degli utilizzatori di strumenti di calcolo portatili, di poter usufruire degli stessi servizi di networking a disposizione degli utenti di sistemi fissi.

Esiste infine un terzo fattore, molto sentito in Italia, che è l'elevato costo di realizzazione dei sistemi di cablaggio in particolari edifici, ad esempio quelli storici, soggetti alla tutela del Ministero dei Beni Culturali.

La fattibilità delle reti locali wireless è oggigiorno possibile grazie ai forti progressi nei settori delle tecnologie dei semiconduttori (chip all'arseniuro di gallio), delle alte frequenze (microonde) e ottiche (infrarossi).

Le reti per trasmissione dati non cablate si possono classificare in due diverse categorie, a seconda delle loro dimensioni e dei servizi ed applicazioni offerti all'utenza, esattamente come nel caso delle loro controparti cablate:

- wide area wireless data network o *wireless WAN*, progettate per la trasmissione di dati su base metropolitana o nazionale, con velocità nel range 2.4 - 19.2 Kb/s;
- local area wireless data network o *wireless LAN*, progettate per l'utilizzo in ambienti di dimensioni ridotte all'interno di edifici, con velocità da 230 Kb/s a 10 Mb/s.

11.2 EVOLUZIONE DELLE LAN CABLATE

La definizione di rete locale data nel paragrafo 5.1 prevede l'esistenza di un unico mezzo trasmissivo ad alta velocità e basso tasso di errore la cui capacità

trasmissiva sia condivisa da tutte le stazioni collegate, in modo simile a quanto schematizzato nella parte sinistra di figura 11.1. Tale modello rispecchia fedelmente la struttura di una rete Ethernet cablata con cavo coassiale o quella di una rete Token Ring cablata su un concentratore passivo.

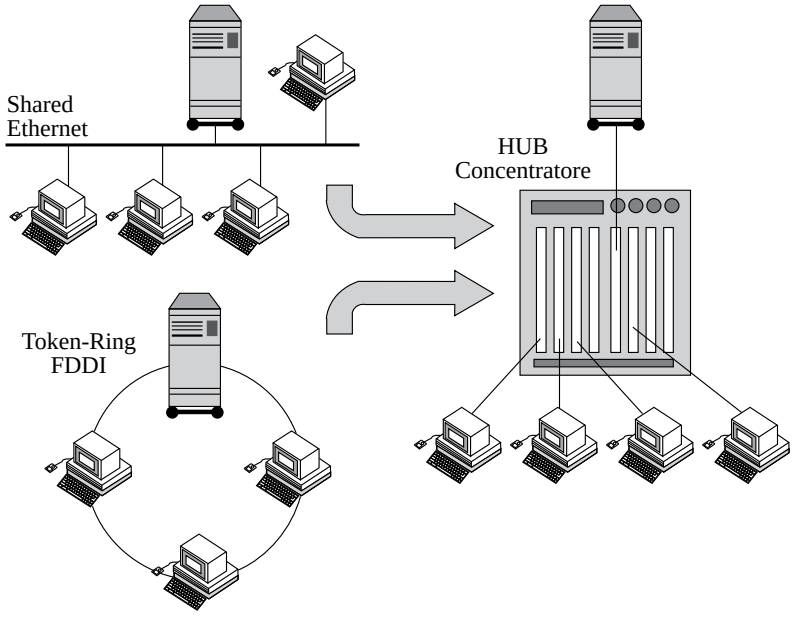


Fig. 11.1 - Evoluzione delle LAN cablate.

Abbiamo altresì visto nel capitolo 4 come gli standard relativi al cablaggio strutturato degli edifici abbiano ricondotto tutte le LAN ad una topologia sostanzialmente stellare, in cui i cavi collegano le stazioni a dei concentratori (HUB) che fungono da centro stella, come schematizzato nella parte destra di figura 11.1.

La topologia stellare non introduce benefici in termini di capacità trasmissiva globale della rete se i concentratori si comportano come ripetitori (nel caso di Ethernet) o semplici centro stella (nel caso di reti ad anello): infatti in tali casi il concentratore continua ad avere una capacità trasmissiva totale pari a quella del singolo cavo.

Nella topologia stellare è però possibile sostituire i concentratori con commutatori di trame di livello MAC, comunemente detti switch (figura 11.2), caratterizzati da una capacità trasmissiva globale molto superiore a quella dei singoli cavi: uno switch, infatti, è in grado di permettere la trasmissione contemporanea di più pacchetti se i mittenti e i destinatari sono diversi.

Se, per esempio, lo switch ha una capacità trasmissiva di 160 Mb/s e il numero di stazioni collegate è 32 allora i 10 Mb/s di Ethernet diventano effettivamente disponibili per ciascuna singola stazione: 10 Mb/s per ognuna delle 16 possibili coppie. Il 10BaseT si trasforma in un protocollo punto-punto tra stazione e switch e ogni singolo cavo stazione-switch diviene un dominio di collisione separato.

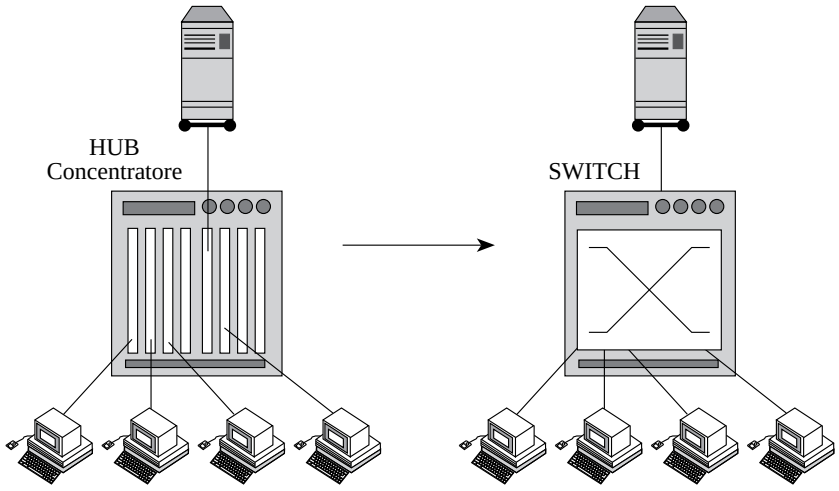


Fig. 11.2 - Dal concentratore allo switch.

Se si ritiene che i 10 Mb/s disponibili per ogni stazione siano insufficienti, oppure si vogliono fornire prestazioni molto elevate anche quando le stazioni siano collegate su switch diversi, è indispensabile ricorrere a protocolli a più elevate prestazioni, sia per i collegamenti tra stazione e switch, sia per i collegamenti di dorsale, cioè tra switch e switch.

Uno schema delle evoluzioni possibili è mostrato in figura 11.3.

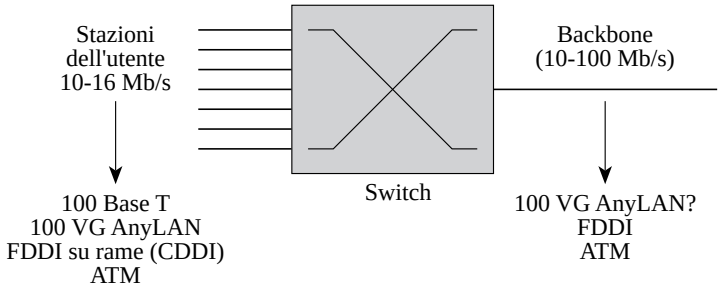


Fig. 11.3 - Evoluzione dei collegamenti.

Per quanto concerne i collegamenti tra stazioni e switch la scelta più semplice consiste nell'adottare una rete locale a 100 Mb/s. Le scelte possibili sono tre: 100BaseT, 100VG AnyLAN e FDDI su rame (anche detto CDDI o, più propriamente TP-PMD). Nessuna di queste tre reti implica cambiamenti a livello di gestione dei protocolli rispetto al 10BaseT in quanto sono tutte perfettamente inserite nel progetto IEEE 802. Le prime due (100BaseT e 100VG AnyLAN), inoltre, sono anche in grado di operare sugli stessi cavi di categoria 3 (si veda il capitolo 3) impiegati per 10BaseT, mentre CDDI richiede necessariamente un cablaggio in categoria 5.

L'adozione di ATM per il collegamento tra stazioni e switch, oltre a richiedere un cablaggio in fibra ottica o in cavo di rame di categoria 5, pone ulteriori problemi in quanto ATM non è inserito nel progetto IEEE 802 e quindi le funzionalità tipiche delle LAN devono essere emulate tramite opportuno software.

Diverso è il discorso per i collegamenti di dorsale, dove 100BaseT risulta inadatto per problemi di lunghezza massima dei collegamenti. 100VG AnyLAN è invece teoricamente utilizzabile, anche se le uniche due architetture ampiamente diffuse sono FDDI e ATM.

FDDI ha il vantaggio di essere inserito nel progetto IEEE 802, di avere standard consolidati da tempo e ottima interoperabilità in ambiente multivendor, anche se le prestazioni massime sono limitate a 100 Mb/s (200 Mb/s nel caso di FDDI full duplex).

ATM ha il vantaggio di poter crescere sino a 2.4 Gb/s e oltre, non avendo limiti significativi di banda sulle fibre ottiche delle dorsali, ma soffre ancora di problemi di "gioventù" (scarsa interoperabilità multivendor) e richiede comunque una estensione per emulare le funzionalità delle reti locali.

Nel seguito di questo capitolo verranno descritte le possibili evoluzioni della rete Ethernet 10BaseT e gli standard 100BaseT e 100VG AnyLAN, mentre per FDDI si rimanda il lettore al capitolo 8 e per ATM ai capitoli 19, 20 e 21.

11.3 ETHERNET SWITCHING

Il termine *Ethernet switching* indica una rete Ethernet in cui sono presenti degli switch in luogo dei concentratori. Gli Ethernet switch sono a tutti gli effetti dei bridge (si veda il capitolo 10) con una porta dedicata verso ogni stazione e un buon rapporto prestazioni/prezzo. In funzione del fornitore e della politica commerciale a volte possono essere sprovvisti della possibilità di impostare entry statiche nel filtering database o dell'algoritmo di spanning tree (non indispensabile in quanto lavorano tipicamente su topologie stellari).

Il primo prodotto Ethernet switching a comparire sul mercato è il prodotto

Kalpana integrato anche negli hub della SynOptics. Questo prodotto, quando opera in ambiente omogeneo Ethernet a 10 Mb/s, introduce una variante significativa all'algoritmo di bridging. Infatti, quando riceve una trama MAC (per semplicità detta pacchetto nel seguito) esamina immediatamente l'indirizzo di destinazione, consulta le sue tabelle di instradamento per determinare la porta di destinazione e, se questa è libera, inizia a ritrasmettere il pacchetto mentre lo sta ancora ricevendo (modalità *cut-through*).

Uno switch, quando opera in modalità cut-through, non può verificare e ricalcolare la FCS prima di aver iniziato la ritrasmissione della trama (poiché la FCS è posizionata in coda al pacchetto) e quindi, contrariamente ai bridge, non può evitare di inoltrare sulla rete il singolo pacchetto corrotto; può tuttavia effettuare misure statistiche al fine di disabilitare la modalità cut-through sulle porte con elevato tasso di errore.

Esistono altre quattro condizioni che inibiscono il cut-through e impongono allo switch di operare in modalità store-and-forward come i bridge:

- quando uno switch opera tra due reti locali appartenenti a due standard diversi (per esempio Ethernet e FDDI);
- quando uno switch opera tra due reti identiche, ma a velocità diverse (per esempio Token Ring a 4 e 16 Mb/s);
- quando la porta di destinazione è occupata;
- quando il pacchetto ha un indirizzo di destinazione multicast o broadcast.

Inoltre, quando la trama è corta, il vantaggio di tale tecnica è trascurabile rispetto allo store-and-forward.

Il vantaggio principale nell'evitare uno store and forward dell'intero pacchetto risiede nella riduzione del tempo di latenza rispetto ai bridge; lo svantaggio è quello di ritrasmettere eventuali pacchetti corrotti.

Questo approccio è stato utilizzato dalla SynOptics nel modulo 3328 (*Ethernet switching engine module*) che è dotato di 6 porte, di cui una si collega a uno dei canali sul bus dell'hub e cinque sono porte esterne RJ45.

Con 6 porte ci possono essere, ad un dato istante, al massimo 3 trasmissioni in corso, per cui la capacità trasmissiva totale massima è di 30 Mb/s.

Anche la Chipcom propone un prodotto analogo con il modulo 5106I-S (*Ethernet switching module*), senza però utilizzare la tecnologia Kalpana. Questo modulo, illustrato in figura 11.4, ha un filtering rate globale di 90.000 pps (pacchetti per secondo) e un forwarding rate aggregato di 42.000 pps. La gestione avviene tramite una porta di console RS-232 o tramite protocolli SNMP/MIB II. La Chipcom rende disponibili anche i moduli 5106I-B e 5106I-R che sono simili,

ma dotati rispettivamente di software di bridging o di brouting.

Questi moduli hanno in totale 8 porte, di cui:

- 3 dal lato backplane, che possono essere connesse ai 3 canali Ethernet dell'hub;
- 5 esterne, di cui 3 con RJ45 e 2 con AUI.

Sono attivabili contemporaneamente soltanto 6 porte, per cui ci possono essere al massimo 3 trasmissioni in corso, quindi la capacità trasmissiva totale massima è di 30 Mb/s, come nel caso precedente.

La soluzione Chipcom ricalca molto più l'architettura dei bridge di quella SynOptics: infatti il modulo Chipcom realizza uno store and forward completo del pacchetto, con controllo ed eventuale ricalcolo della FCS. Questo permette di operare in modo più affidabile anche tra reti con MAC diversi, ma aumenta di conseguenza il tempo di latenza specialmente per i pacchetti lunghi, in cui il tempo di store-and-forward è dominante sul tempo necessario per decidere dove ritrasmettere il pacchetto.

La possibilità di utilizzare la tecnologia switching è stata introdotta anche per FDDI: Digital Equipment Corp. ha immesso sul mercato un apparato FDDI switching detto Gigaswitch che ha un funzionamento molto simile a quella degli Ethernet switch.

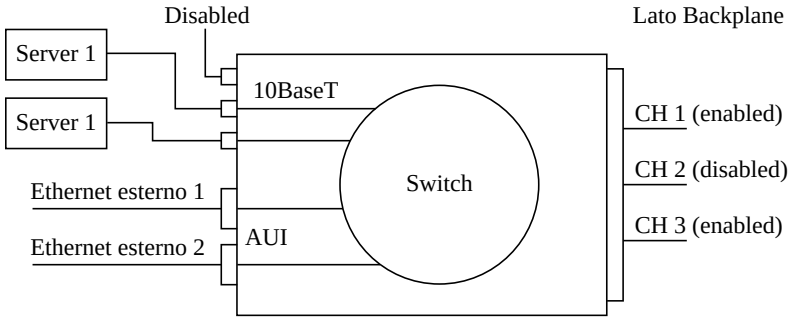


Fig. 11.4 - Chipcom 5106I-S: esempio di switch Ethernet.

11.4 ETHERNET DEDICATO

La connessione punto-punto tra stazioni e schede Ethernet switching su hub è una soluzione valida in attesa di tecnologie più veloci e assume molto spesso il nome di Ethernet dedicato o *personal Ethernet*. Il vantaggio risiede nella disponibilità di una capacità trasmissiva dedicata di 10 Mb/s, molto spesso più che sufficiente per la maggior parte delle applicazioni, a costi ragionevoli.

Occorre qui ricordare che i collegamenti Ethernet punto-punto sono per loro natura half-duplex, cioè non sono in grado di consentire la trasmissione contemporanea nelle due direzioni. In tali collegamenti le collisioni si possono verificare solo tra la stazione e lo switch e servono appunto a gestire la natura half-duplex del collegamento.

I primi moduli Ethernet switching erano stand-alone e quindi confinavano la tecnica switching all'interno di un singolo hub: per distribuirla su più hub è necessario che il trasporto sulla tratta hub-hub abbia prestazioni superiori (ad esempio usando FDDI).

All'inzio del 1992 è apparsa sul mercato una prima soluzione con il sistema FX 8610 della Fibronix, che è praticamente un bridge FDDI-Ethernet multiporta a basso costo, comprendente da 2 a 12 porte Ethernet full speed.

I moduli Ethernet hanno 2 porte e possono essere 10BaseT o 10Base2 (al massimo 4 nodi per cavo coassiale). Una connessione ad una porta 10BaseT viene considerata collision-free (priva di collisioni), quella ad una porta 10Base2 collision-less (con bassa probabilità di collisione).

Questa soluzione, illustrata in figura 11.5, ha tempi di latenza di 0.2 ms tra due porte Ethernet dello stesso bridge e di 0.5 ms tra due porte Ethernet di bridge diversi.

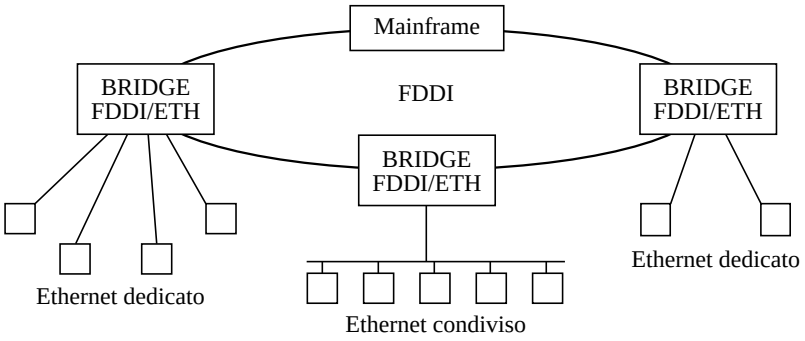


Fig. 11.5 - Ethernet dedicato.

Verso la fine del 1993 la Chipcom ha proposto un'interessante soluzione con due prodotti facenti parte di una medesima famiglia: lo StarBridge Turbo Switch ed il Galactica Network Switching Hub, che sono di fatto dei bridge multiporta di tipo full-speed, che si differenziano tra loro per la differente flessibilità e costo (figura 11.6).

Lo StarBridge Turbo Switch ha una capacità trasmissiva di 40 Mb/s (molto spesso i costruttori indicano la capacità complessiva di I/O che è pari al doppio della capacità

trasmissiva, in questo caso 80 Mb/s) ed è composto da 8 porte Ethernet. Esso può essere interconnesso ad un altro bridge della stessa famiglia con due link a 10 Mb/s configurati in modo da lavorare l'uno soltanto in trasmissione ed l'altro solo in ricezione (modalità full-duplex, si veda il paragrafo 11.4.1). In questa modalità si ottiene un collegamento a 20 Mb/s.

Il prodotto Galactica ha una capacità trasmissiva di 160 Mb/s e le configurazioni massime ammesse sono:

- 32 porte (impiegando 4 moduli da 8 porte);
- 24 porte Ethernet ed una porta FDDI (impiegando 3 moduli Ethernet da 8 porte e un modulo FDDI).

Questo prodotto, oltre a poter disporre di una dorsale FDDI per il trasporto hub-to-hub (figura 11.7), offre le seguenti caratteristiche:

- ogni porta può avere fino a 1024 nodi connessi;
- le porte possono essere raggruppate in domini (reti locali virtuali);
- è previsto in futuro un utilizzo di ATM in alternativa a FDDI.

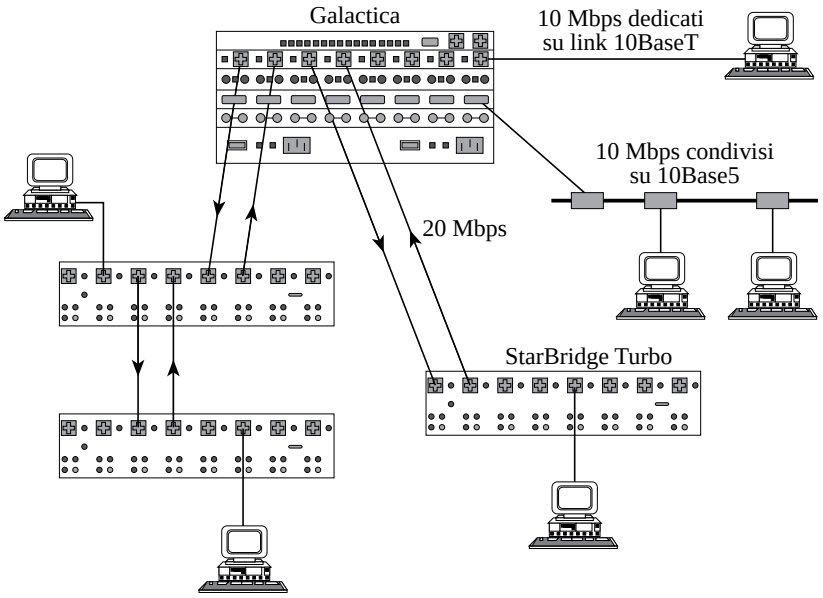


Fig. 11.6 - Connessione tra Galactica e StarBridge.

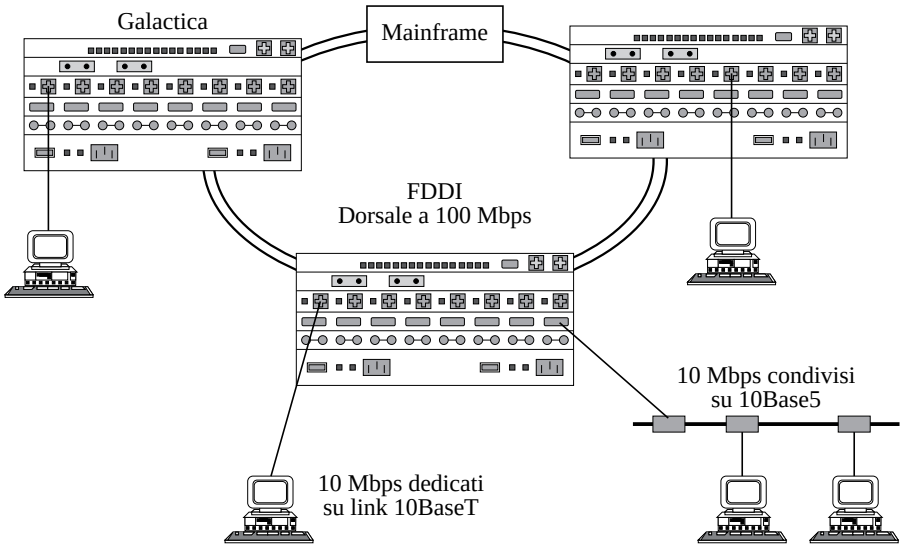


Fig. 11.7 - Dorsale FDDI con i Bridge Galactica.

11.4.1 Ethernet dedicato full-duplex

Per la comunicazione punto-punto tra due bridge o due switch è possibile utilizzare due canali Ethernet classici (half-duplex) in parallelo, ciascuno in modo monodirezionale, ottenendo un canale Ethernet dedicato full-duplex. Questi sono dei canali molto particolari in quanto non soggetti a collisione (in ogni direzione c'è una sola stazione che può trasmettere e quindi per definizione non può collidere con nessun'altra) e quindi i limiti di distanza non sono più dettati dal livello MAC, ma solo dal livello Fisico. La soluzione full-duplex è utilizzabile sia in associazione allo standard 10BaseT che al 100BaseT. Le distanze massime ammesse sono tipicamente di 100 m su cavo UTP, 2 Km su fibra ottica multimodale e 50 Km su fibra otttica monomodale.

11.5 RETI LOCALI VIRTUALI

La tecnologia delle reti locali virtuali (*Virtual LAN* o VLAN) fa riferimento alla capacità offerta dagli switch e dai router di configurare più reti logiche sopra un'unica rete locale fisica. Ogni Virtual LAN è costituita da un insieme di segmenti di rete locale che possono comprendere una singola stazione (segmenti punto-

punto) o un gruppo di stazioni (segmenti condivisi). Le stazioni appartenenti ad una VLAN sono logicamente interconnesse a livello Data Link, anche se fisicamente sono collegate su segmenti diversi. Operando unicamente a livello di centro di gestione della rete è possibile creare più domini, cioè più reti locali virtuali, su una infrastruttura trasmissiva comune senza alcun intervento a livello Fisico.

La possibilità di creare reti locali virtuali da assegnare ai vari gruppi di lavoro permette un'elevata flessibilità in quanto non è necessario che i componenti di un gruppo occupino spazi fisicamente contigui. I vantaggi principali che si ottengono da tale assegnazione derivano dall'isolamento del traffico dei vari gruppi di lavoro al livello Data Link. Questo non solo è importante per ragioni di sicurezza e riservatezza dei dati, ma anche perchè consente di mantenere separato il traffico di multicast/broadcast delle diverse reti virtuali.

L'interoperabilità tra le reti virtuali è garantita da una unità di internetworking esterna, normalmente un router.

La figura 11.8 mostra un esempio di creazione di domini.

Molti costruttori propongono sui loro hub di fascia alta la possibilità di creare e gestire più domini separati: tale capacità è spesso limitata ad un solo hub e quindi non molto utile. Per rendere veramente utile il concetto di rete locale virtuale occorre permettere che un dominio possa includere porte appartenenti ad hub diversi (figura 11.9), i quali naturalmente devono essere interconnessi da una dorsale ad alta velocità.

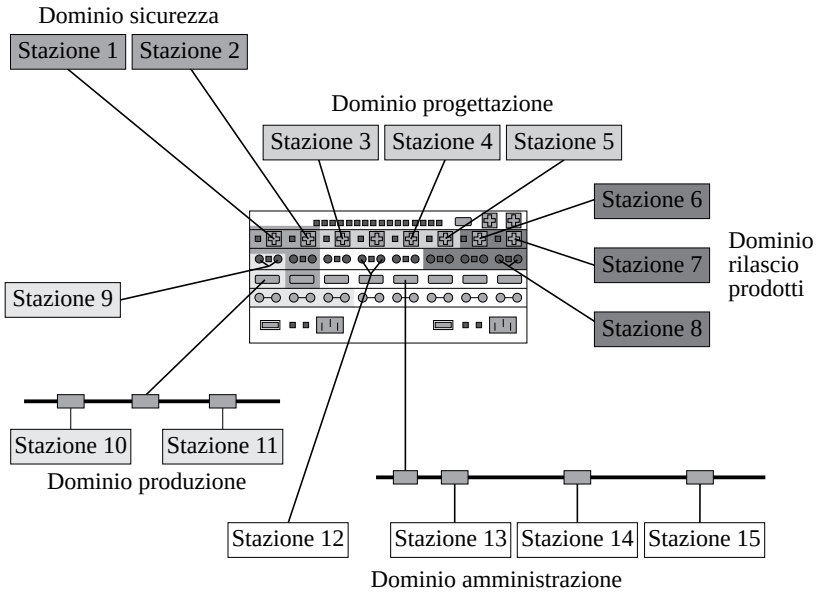


Fig. 11.8 - Creazione dei domini su un singolo hub.

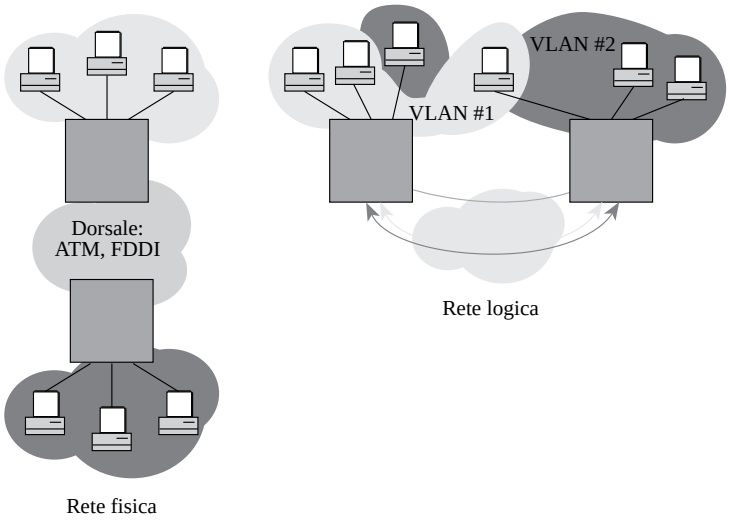


Fig. 11.9 - Creazione dei domini su più hub interconnessi.

Soluzioni di questo tipo iniziano ora ad essere presenti sul mercato: ciò che è ancora carente è la possibilità di avere interoperabilità multivendor, cioè di disporre di una modalità standard per identificare a livello di dorsale l'appartenenza dei pacchetti alle diverse reti locali virtuali.

La Cisco System Inc. adotta per la sua famiglia Catalyst lo standard IEEE 802.10 (SDE: Secure Data Exchange) per marcare i pacchetti appartenenti ai vari domini prima di trasmetterli sulla dorsale FDDI. Tale standard si occupa di problemi legati alla sicurezza nelle LAN e nelle MAN, problemi derivanti in primo luogo dalla trasmissione in broadcast (fisicamente sui bus, logicamente sugli anelli) dei pacchetti. Qualsiasi stazione può ascoltare il traffico altrui, alterarlo, o generarne di illecito. Tra i vari problemi esiste anche quello dell'identificazione sicura di una stazione e del riconoscimento di essa come appartenente ad un gruppo (sottorete) all'interno del quale è ammesso lo scambio di pacchetti. Lo standard IEEE 802.10 fornisce a livello di SDE-PDU un meccanismo per identificare pacchetti appartenenti a sottoreti diverse tramite un campo di 4 byte detto "VLAN ID" nell'header del pacchetto 802.10. Quando una trama MAC deve essere inoltrata sul backbone, acquisisce un header 802.10 contenente il VLAN ID del segmento che lo ha generato. Lo switch o il router che riceve il pacchetto dal backbone verifica il VLAN ID e quindi invia la trama, privata dell'header 802.10, alle porte che appartengono alla stessa VLAN.

Quando il prodotto Catalyst è adottato in associazione ad un backbone ATM

non si usa lo standard IEEE 802.10, bensì il supporto per le Virtual LAN che è previsto nello standard ATM Forum LAN Emulation, descritto nel capitolo 20.

11.6 ETHERNET A 100 Mb/s

Sviluppata ormai 20 anni fa, Ethernet è una delle tecnologie di rete più standard e assestate esistenti sul mercato. L'idea di avere una rete Ethernet a 100 Mb/s è da lungo tempo vagheggiata e non realizzata in quanto nel MAC di Ethernet (e di IEEE 802.3) la velocità non è un parametro indipendente, ma è legato indissolubilmente ad altri due: la lunghezza minima del pacchetto e il round trip delay (si veda il paragrafo 6.5.2). Il round trip delay determina l'estensione del dominio di collisione e quindi la lunghezza massima della rete.

Se si vuole realizzare una rete Ethernet a 100 Mb/s bisogna modificare la velocità unitamente ad almeno uno degli altri due parametri: poiché la velocità sale di un fattore 10, uno degli altri due parametri deve modificarsi analogamente di un fattore 10. Una possibile alternativa è quella di cambiare l'algoritmo del MAC, con i vantaggi e gli svantaggi che questa rilevante modifica comporta.

Nel 1992 sono state presentate due proposte per Ethernet a 100 Mb/s: Grand Junction Networks ha messo in campo la sua tecnologia basata su CSMA/CD e HP e AT&T le hanno risposto con la loro tecnologia basata su un nuovo metodo di accesso detto Demand Priority. Alla fine del '92 le due proposte sono state portate all'attenzione dell'IEEE per concorrere a diventare lo standard ufficiale per "Fast Ethernet". Tuttavia, vista la loro totale inconciliabilità, l'IEEE non è riuscita a decidersi e nel luglio '93 ha affidato le due tecnologie a due comitati di standardizzazione differenti: la proposta di HP e AT&T, nota anche come 100BaseVG (Voice Grade), è stata affidata al comitato 802.12, mentre quella CSMA/CD, conosciuta come 100BaseX, è stata affidata al sottocomitato 802.3u.

Poco dopo IBM si è alleata con HP per fornire la sua collaborazione nelle fasi di sviluppo e promozione di uno standard congiunto e, quindi, ha annunciato alla stampa il supporto di Token Ring da parte di 100BaseVG che da quel momento ha preso il nome di 100VG AnyLAN.

In quello stesso periodo sono state create dai due fronti opposti la Fast Ethernet Alliance (FEA) e il 100VG AnyLAN Forum (VGF) per sveltire il processo di standardizzazione delle rispettive tecnologie. Mentre i membri del VGF crescevano in numero e in importanza (seguendo l'esempio di IBM, anche Cisco nel novembre '94 si è unita alla cordata guidata da HP), i concorrenti appartenenti alla FEA rilasciarono lo standard per Fast Ethernet con il nome di 100BaseT. In esso era stata aggiunta alla bozza originale una variante dal nome prima di 4T+ e poi di

T4, basata su UTP di categoria 3 a quattro coppie, ed era stata definita la Media Independent Interface (MII), ossia una AUI (Attachment Unit interface) aggiornata per i 100 Mb/s. Per coordinare i test di interoperabilità tra i prodotti 100BaseT, i membri della FEA hanno poi fondato il Technology Research Interoperability Lab.

La situazione all'inizio del 1995 vede nel novero dei sostenitori di 100BaseT: 3Com Corp., Intel Corp., Digital Equipment Corp., Bay Networks, Grand Junction Networks, Cabletron Systems, National Semiconductor, Sun Microsystems, Standard Microsystems Corp., Hitachi Cable, Asanté Technologies; in tutto una sessantina di costruttori.

Tra i sostenitori di 100VG AnyLAN spiccano: Hewlett-Packard Co., AT&T Microelectronics, IBM Corp., Cisco, Proteon, Ungermann-Bass, Thomas-Conrad.

Occorre ancora sottolineare che la situazione è attualmente tutt'altro che stabile: 3Com, per esempio, ha presentato all'inizio del '95 una tecnologia, nota come PACE (Priority Access Control Enabled), che permette di superare i problemi di temporizzazione di Ethernet, riuscendo a dedicare a una connessione una larghezza di banda costante definibile dall'utente.

11.6.1 100Base-T

100BaseT o IEEE 802.3u è l'unica LAN che possa definirsi "Ethernet a 100 Mb/s", poiché mantiene inalterato il classico algoritmo CSMA/CD implementato su 10BaseT, operando però a 100 Mb/s. La dimensione minima del pacchetto non è stata alterata e si è quindi dovuto ridurre di un fattore 10 il round trip delay e quindi il diametro della rete. Questo ha imposto la revisione di numerosi parametri ad esso collegati.

In 100BaseT i valori fissati per i principali parametri sono:

- velocità trasmissiva 100 Mb/s;
- bit time 10 ns;
- Inter Packet Gap (IPG) 0.96 μs;
- slot time 512 bit, cioè 5.12 μs.

100BaseT usa l'interfaccia esistente del livello MAC IEEE 802.3 e la connette attraverso uno strato chiamato *Media Independent Interface* (MII) a una famiglia di sublayer fisici che comprende: 100BaseT4 PHY, 100BaseTX PHY e 100BaseFX PHY.

Il duo TX/FX (anche chiamato 100BaseX) si basa sul substrato physical medium dependent di FDDI (si veda il paragrafo 8.6.4) e trasmette, con la codifica 4B5B a 125 Mb/s, su 2 coppie UTP di categoria 5 o su 2 coppie STP type 1 (variante

TX), oppure su due fibre multimodali (variante FX).

100BaseT4, invece, usa un nuovo livello fisico per la trasmissione su doppino a 4 coppie di categoria 3 o superiore. Il collegamento tra stazione e repeater usa, delle quattro coppie, due in modalità half duplex, cioè alternativamente in trasmissione o in ricezione, una sempre in trasmissione ed una sempre in ricezione (figura 11.10). La trasmissione avviene quindi su tre coppie contemporaneamente. La quarta coppia, in ricezione, serve per permettere all'interfaccia fisica di rilevare la presenza di collisioni senza dover introdurre complicazioni aggiuntive al protocollo MAC rispetto allo standard IEEE 802.3.

Per trasmettere i pacchetti su 3 coppie si utilizza una codifica codifica di tipo 8B6T (paragrafo 3.1.3). Essa suddivide un flusso binario a 100 Mb/s in tre flussi da 25 Mbaud (simboli, in questo caso ternari, al secondo). Infatti, trasmettere 100 Mb/s divisi su tre canali significa trasmettere $100/3 = 33.\overline{3}$ Mb/s su ogni canale, e trasformare ogni ottetto in sei simboli ternari significa associare ad ogni simbolo un'informazione pari ad 8/6 di bit; quindi su ogni canale è necessario trasmettere $33.\overline{3} : (8/6) = 25$ Mbaud. Nel caso peggiore, relativamente alla massima frequenza di trasmissione, si ottiene una sequenza alternata di simboli "+" e "-", che dà luogo ad una frequenza fondamentale di 12.5 MHz.

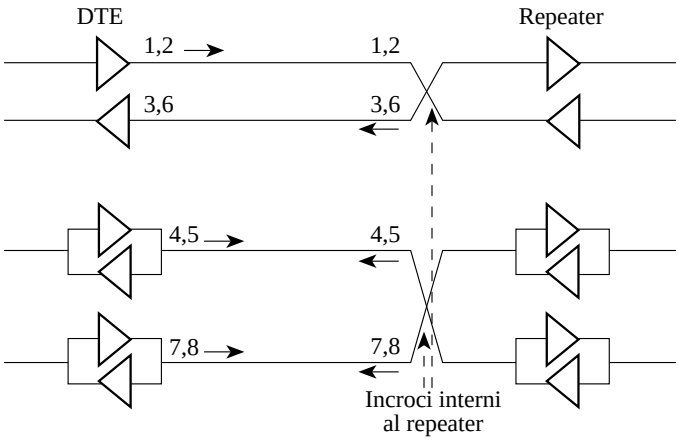


Fig. 11.10 - 100BaseT4: uso delle coppie.

In questo schema trasmissivo partendo da 8 bit, che consentono 256 possibili combinazioni diverse di valori, si codificano 6 simboli ternari, che consentono di rappresentare 729 valori, e questo permette l'introduzione di informazioni aggiuntive per la sincronizzazione del flusso trasmissivo e per il controllo degli errori.

Nelle prime bozze di standard la mappa delle varianti di 100BaseT si presentava come in figura 11.11 (in cui sono state riportate anche 100VG AnyLAN e FDDI per confronto) in cui si nota che 100BaseX comprende i sottostrati TP-PMD e PMD su fibra di FDDI.

La necessità di uno standard più omogeneo ha portato il comitato 802.3u a definire nelle bozze conclusive una architettura più compatta, come appare nelle figure 11.12 e 11.13.

Il *Reconciliation Sublayer* (RS) fornisce la funzione di traduzione dei segnali a livello MII in primitive di servizio PLS (*Physical Layer Signaling*). Il PLS è un sottostrato del Physical Layer del modello OSI ed è responsabile della codifica/decodifica dei dati in fase di trasmissione e di ricezione. In 10BaseT è collocato tra la AUI e il MAC (figura 6.24) e usa la codifica Manchester.

La Medium Independent Interface (MII) fornisce un'interconnessione semplice ed economica tra il MAC e i diversi sottostrati fisici (PHY) e tra i PHY e le entità di *STAtion management* (STA). Essa è in grado di funzionare sia a 10 Mb/s che a 100 Mb/s attraverso canali di ampiezza pari a 4 bit (nibble wide). Sun Microsystems è stato uno dei primi costruttori a presentare una scheda basata sulla soluzione MII più MAU esterna.

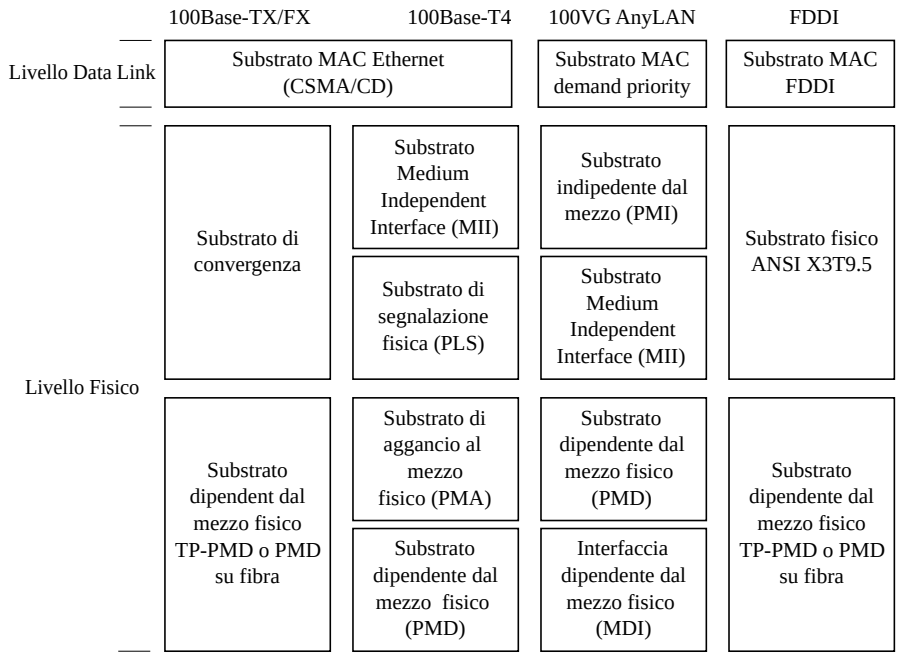

100Base-TX/FX
100Base-T4
100VG AnyLAN
FDDI
Livello Data Link
Substrato MAC Ethernet (CSMA/CD)
Substrato MAC demand priority
Substrato MAC FDDI
Livello Fisico
Substrato di convergenza
Substrato Medium Independent Interface (MII)
Substrato indipedente dal mezzo (PMI)
Substrato fisico ANSI X3T9.5
Substrato di segnalazione fisica (PLS)
Substrato Medium Independent Interface (MII)
Substrato dipendent dal mezzo fisico TP-PMD o PMD su fibra
Substrato di aggancio al mezzo fisico (PMA)
Substrato dipendente dal mezzo fisico (PMD)
Substrato dipendente dal mezzo fisico (PMD)
Interfaccia dipendente dal mezzo fisico (MDI)
Substrato dipendente dal mezzo fisico TP-PMD o PMD su fibra

Fig. 11.11 - Schema a blocchi delle varianti 100BaseT.

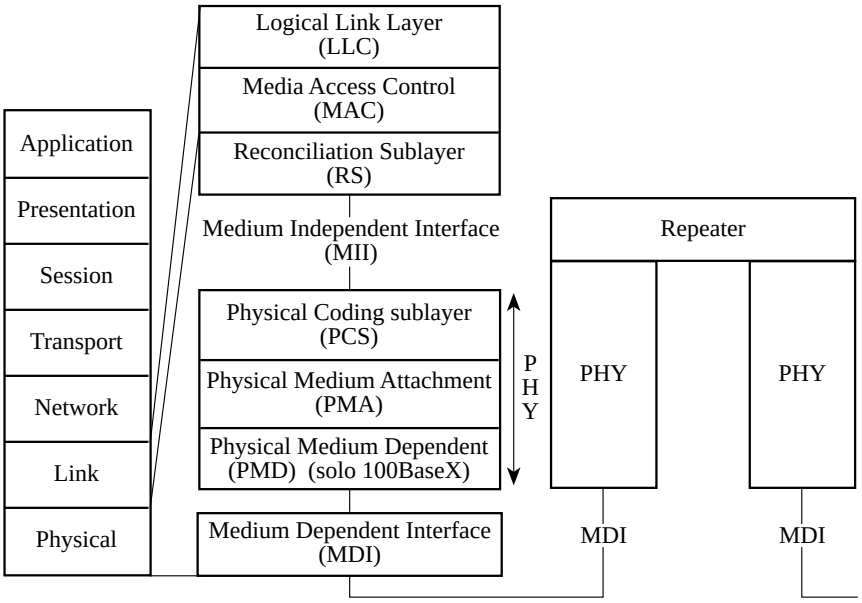


Fig. 11.12 - 100BaseT: relazione con il modello di riferimento ISO OSI.

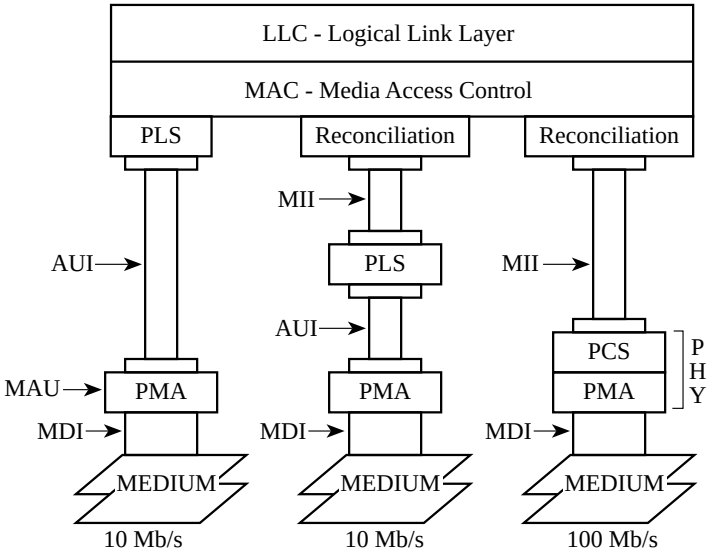


Fig. 11.13 - Architettura di 100BaseT.

Il sottolivello *Physical Layer Device* (PHY) è la porzione del livello fisico tra l'MDI (Medium Dependent Interface) e la MII che comprende i sottostrati *Physical Coding Sublayer* (PCS), *Physical Medium Attachment* (PMA) e, se presente, Physical Medium Dependent (PMD).

Il PCS è usato in 100BaseT per accoppiare la MII con il PMA. Il PCS contiene le funzioni per codificare i bit di dati in *code groups* (insiemi di sei simboli ternari per la variante T4; insiemi di cinque bit di codice per le varianti TX e FX) che possono essere trasmessi sul mezzo fisico. Sono definite due strutture PCS per 100BaseT: una per 100BaseX che usa la codifica 4B5B per generare un flusso full-duplex a 125 Mb/s, e una per 100BaseT4 che codifica i nibble di dati ricevuti dalla MII in "code groups" di tipo 6T usando uno schema di codifica 8B6T.

Il sottolivello PMA è la porzione del livello fisico che contiene le funzioni per la trasmissione, ricezione, clock recovery e skew alignment.

Il sottolivello *Physical Medium Dependent* (PMD) è la porzione del livello fisico responsabile dell'interfaccia con il mezzo trasmissivo.

La *Medium Dependent Interface* (MDI) è l'interfaccia meccanica ed elettrica tra il mezzo trasmissivo e il PMA.

Lo schema dell'utilizzo delle coppie 100BaseTX e 100BaseT4 è mostrato in figura 11.14.

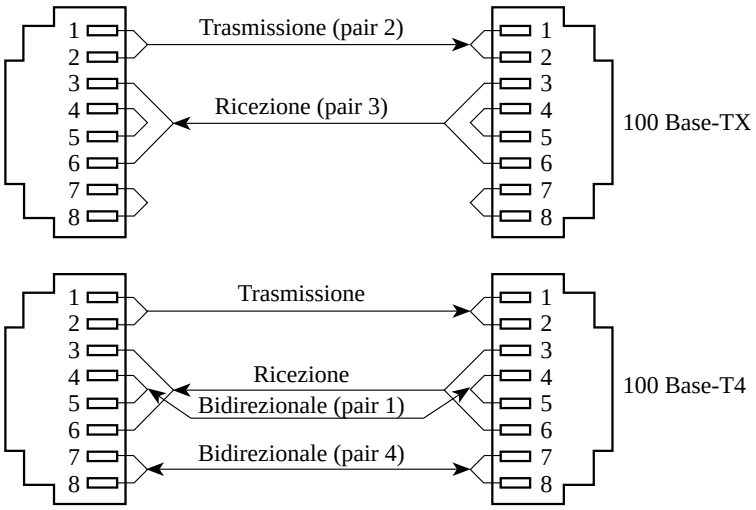


Fig. 11.14 - Utilizzo delle coppie nelle due varianti TX e T4.

Le possibili modalità di funzionamento di una scheda 100BaseT previste nello

standard sono: 100BaseT4, 100BaseX full o half duplex, 10BaseT full o half duplex. La modalità full duplex è interessante per il collegamento tra switch in quanto consente di realizzare collegamenti dedicati a 20 o 200 Mb/s.

I prodotti attualmente in commercio sono in grado di funzionare secondo quasi tutte queste modalità; in più gli hub offrono sia porte condivise sia porte dedicate, sulle quali, come già detto, non si verificano collisioni. Un'altra caratteristica importante è la possibilità di impostare, tramite un registro di controllo, il duplex mode, il power consumption state e la gestione della velocità trasmissiva. Quest'ultima può essere negoziata e quindi impostata a 10 o 100 Mb/s a seconda che il dispositivo all'altro capo del link sia di tipo 10BaseT o 100BaseT, permettendo una notevole scalabilità e flessibilità di configurazione.

La capacità di un dispositivo di commutare automaticamente tra le due modalità di funzionamento 10BaseT e 100BaseT è legata a due possibili meccanismi noti come *NWay Auto-Negotiation* e *Auto Sensing*. Sia l'NWay Auto-Negotiation che l'Auto Sensing sono compatibili con gli standard IEEE e permettono a un adattatore 10/100 (cioè con possibilità di funzionamento a 10 e a 100 Mb/s) di funzionare in modalità 10BaseT se connesso a un hub o switch 10BaseT, o in modalità 100BaseT se connesso a un hub o switch 100BaseT. Lo standard IEEE 802.3u descrive la funzione di NWay Auto-Negotiation, opzionale, di cui viene però raccomandata l'implementazione.

Il vantaggio maggiore di un dispositivo che usa l'NWay Auto-Negotiation rispetto a uno che usa l'Auto-Sensing risiede nelle capacità di network management e nella capacità di notifica della modalità di funzionamento full duplex. Per esempio, se una scheda 10BaseT preesistente viene connessa a un hub che funziona solo in modalità 100BaseT, non è possibile alcuna comunicazione tra i due dispositivi dal momento che l'hub 100BaseT non è in grado di funzionare come 10BaseT. L'NWay Auto-Negotiation, tuttavia, avvisa l'applicazione di network management che la connessione non è valida perché l'end node è un dispositivo 10BaseT. Un dispositivo di tipo Auto-Sensing non è invece in grado di indicare all'applicazione di management il motivo per cui la connessione non è valida. Inoltre, l'NWay Auto-Negotiation diventerà il metodo opzionale, standard IEEE, di comunicare la capacità di funzionamento half o full duplex. Attualmente, gli switch 10BaseT che supportano connessioni full duplex usano metodi proprietari di comunicazione tra adattatore e switch. Per essere conformi allo standard le schede e le porte di tali switch dovrebbero usare l'NWay.

L'Auto-Negotiation è effettuata fuori banda usando una sequenza modificata dei segnali di test del collegamento detti link integrity test pulses usati in 10BaseT. L'informazione è trasmessa all'interno di un burst di link integrity test pulse vicini

chiamato un *Fast Link Pulse* (FLP), che viene generato all'accensione, impostato attraverso il network management o attivato mediante l'intervento manuale. I dati estratti dall'FLP informano la stazione ricevente delle capacità del trasmettitore all'altro capo del segmento. Se vengono rilevati degli FLP, l'algoritmo di auto-negoziazione determina il modo di funzionamento con le massime performance comuni, e aggiorna entrambe le estremità del link. Se una delle due estremità del segmento è di tipo 10BaseT, ma non è in grado di generare Fast Link Pulses (come tutte le schede e gli hub 10BaseT esistenti), allora il segmento opererà in modalità 10BaseT. Si possono anche usare le funzionalità offerte dal network management per forzare il modo di funzionamento del segmento a 10BaseT anche quando sarebbe possibile una comunicazione di tipo 100BaseT.

L'Auto-Sensing è un meccanismo più statico: una scheda con l'Auto-Sensing tenta di determinare la velocità dell'hub all'altra estremità del segmento osservando il tipo di Link Integrity Pulses che vengono generati. Una scheda 10/100 con Auto-Sensing invia dei Normal Link Pulses di tipo Fast Ethernet e controlla la risposta da parte dell'altro adattatore. Se all'altro capo del segmento c'è un dispositivo 10BaseT che invia Normal Link Pulses di tipo 10BaseT, allora l'adattatore con Auto-Sensing passerà automaticamente a quella modalità di funzionamento. Se, invece, l'altra estremità del segmento sta generando Fast Ethernet Normal Link Pulses o Fast Link Pulses, allora l'adattatore con Auto-Sensing se ne accorgerà e passerà automaticamente a funzionare come 100BaseT. L'Auto-Sensing è standard ed è in grado di interoperare con qualsiasi dispositivo di tipo sia NWay che non-NWay. Tutte le schede 10/100 comparse per prime sul mercato utilizzano solo l'Auto-Sensing, ma si prevede che in futuro si diffonda l'NWay Auto-Negotiation.

A causa dell'aumento della velocità trasmissiva di un fattore dieci e del mantenimento del protocollo CSMA/CD e del formato dei pacchetti IEEE 802.3, la massima distanza ammessa tra due end node si riduce a circa 210 m (limite comprensivo del ritardo introdotto dal repeater). Questo consente comunque di cablare 100BaseT attorno ad un hub con 100 m di raggio, e quindi 200 m di diametro, e di avere il 5% di tolleranza. Pertanto, 100BaseT è compatibile con gli standard per il cablaggio strutturato.

In figura 11.15 è schematizzata una LAN 100BaseT realizzata su un cablaggio stellare. Ad ogni hub è associato un dominio di collisione di diametro massimo 200 m e i vari hub sono interconnessi mediante bridge o router. L'hub ha funzionalità di multiport repeater e, nel caso di hub modulari, è permesso un intermediate repeater link lungo fino a 10 m per il collegamento dei diversi moduli.

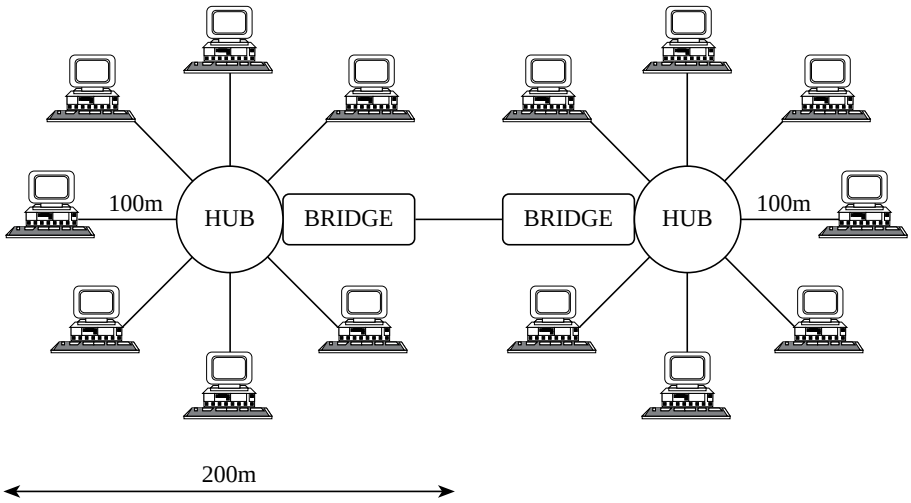


Fig. 11.15 - 100BaseT.

L'obiettivo di 100BaseT è mantenere a livello di schede la compatibilità con 802.3 usando esattamente lo stesso formato di pacchetto, e di avere un posizionamento economico molto interessante: i prodotti 100BaseT dovrebbero costare inizialmente solo il 50% in più degli analoghi prodotti 10BaseT.

11.6.2 100VG AnyLAN

Lo standard 802.12 è anche detto 100VG AnyLAN: "VG" perché è in grado di trasmettere anche su 4 coppie di doppino non schermato di categoria 3, ossia di tipo telefonico o "Voice Grade", "AnyLAN" perché combina la trasmissione di pacchetti Ethernet e Token Ring in un'unica tecnologia. La compatibilità con cavi di categoria 3 è motivata dal fatto che, sebbene tutte le installazioni più recenti siano realizzate con doppino di categoria 5, il doppino "telefonico" è ancora abbastanza diffuso, specialmente nel cablaggio a 25 coppie.

Rispetto ai proponenti il 100BaseT, HP e i suoi alleati hanno creato qualcosa di effettivamente diverso: 100VG AnyLAN mantiene solo il formato del pacchetto 802.3, e sostituisce il MAC a collisione con un MAC *Demand Priority Access Method* (*DPAM*). Grazie a tale protocollo ad ogni porta, e quindi ad ogni stazione di lavoro, viene garantita una minima velocità trasmissiva media (la trasmissione è a 100 Mb/s, ma ogni porta può trasmettere soltanto quando abilitata dall'hub) e

un massimo tempo di ritardo nella risposta (cioè intervallo di tempo tra la richiesta di trasmissione e l'abilitazione ad eseguirla); inoltre il protocollo gestisce due livelli di priorità di trasmissione. Analogamente agli hub tradizionali, la capacità trasmissiva totale su un concentratore 100VG AnyLAN non può superare i 100 Mb/s, ma la possibilità di predefinire il tempo massimo che un pacchetto impiegherà per arrivare al destinatario rende questa tecnologia particolarmente adatta alle applicazioni multimediali.

La scelta di utilizzare quattro coppie di un cavo UTP di categoria 3, invece delle classiche due, non comporta modifiche al cablaggio in quanto gli standard prevedono sempre la posa di almeno due cavi, uno dei quali UTP a quattro coppie.

Le coppie vengono usate in modalità half-duplex, cioè trasmettendo dall'hub al nodo o dal nodo all'hub a seconda delle necessità. Questo permette di trasmettere 100 Mb/s suddividendoli su quattro canali da 25 Mb/s.

In figura 11.16 vediamo come vengano utilizzate le quattro coppie, ognuna delle quali può trovarsi in tre stati (trasmissione, ricezione o contrattazione).

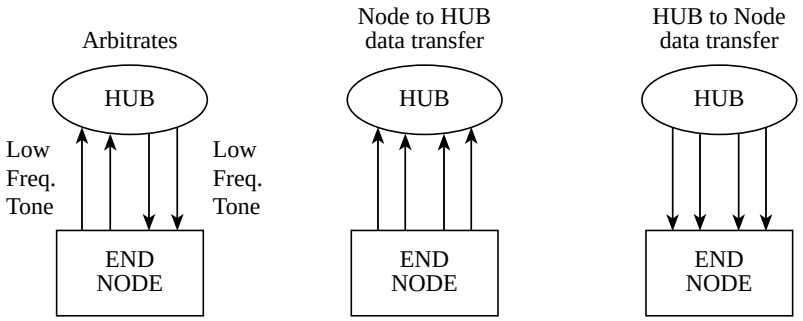


Fig. 11.16 - 100VG AnyLAN: utilizzo di 4 coppie.

La codifica di un pacchetto MAC per la trasmissione sui quattro canali avviene in cinque fasi definite nel sottolivello *Physical Medium Independent* (PMI), qui di seguito descritte e schematizzate nella figura 11.17.

- Nella prima fase, nota come *quintet assembler function*, la sequenza di ottetti di un singolo MAC frame viene suddivisa in quintetti (sequenze di 5 bit). Tale suddivisione può portare ad avere l'ultimo quintetto incompleto, nel qual caso viene completato con bit di valore arbitrario.
- Nella seconda fase, il *quintet streaming*, i quintetti sono assegnati ciclicamente ai quattro canali, iniziando dal primo quintetto, che viene assegnato al canale 0, e terminando quando tutti i quintetti sono stati assegnati.

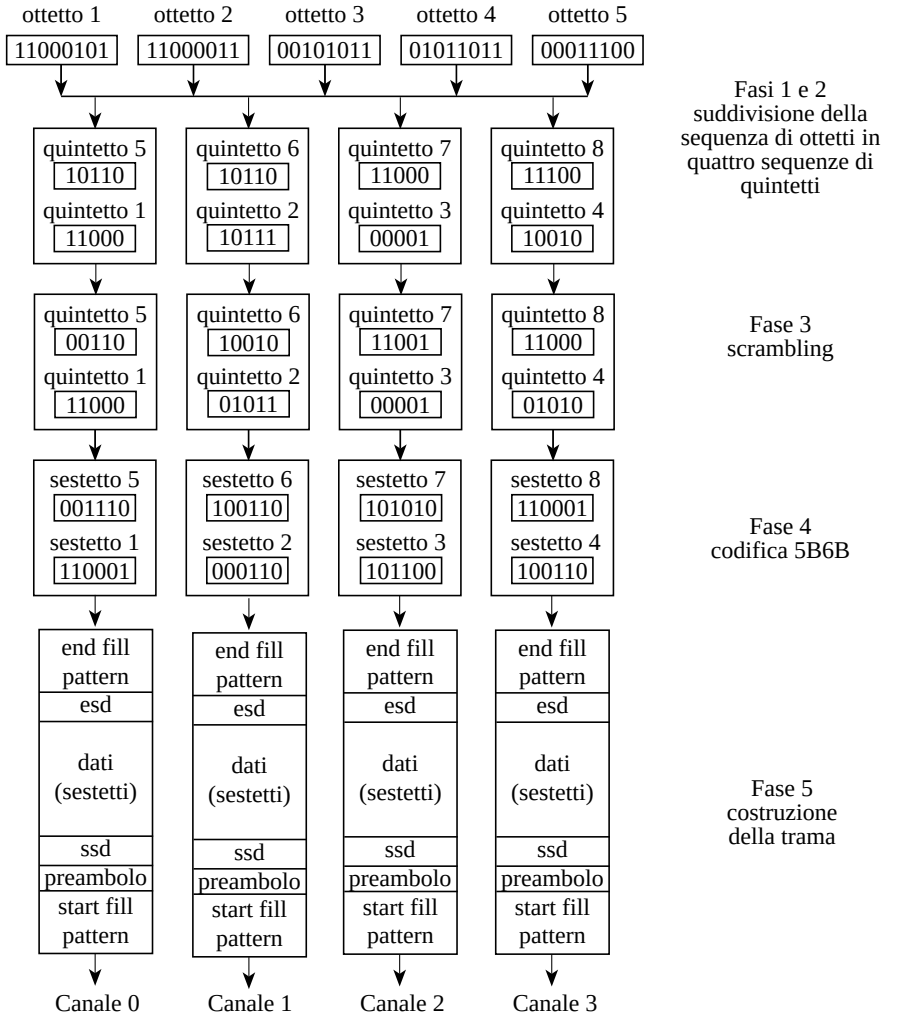


Fig. 11.17 - 100VG AnyLan: codifica.fondamentale del segnale.

- Nella terza fase, chiamata *data scrambling* (o *quintet ciphering*), i quintetti assegnati a ciascun canale vengono modificati tramite una funzione di scrambling (paragrafo 3.1.4). Ogni canale applica lo scrambling indipendentemente e con una chiave differente rispetto agli altri; ciò permette di ridurre le emissioni di disturbi elettromagnetici e quindi la diafonia tra le coppie.

- Nella quarta fase, l'*encoding*, avviene la codifica 5B/6B (paragrafo 3.1.3) in cui ogni quintetto viene codificato con sei bit. L'aggiunta di un bit ogni cinque richiede, per mantenere la velocità trasmissiva prevista al livello Data Link (100 Mb/s), un aumento della velocità sul mezzo fisico pari al 20%, e quindi 30 Mb/s su ogni canale.
- La quinta fase, la *delimiter generator function*, crea, con le sequenze di sestetti in ciascun canale, delle vere e proprie trame, con preambolo, *start of stream delimiter* (ssd), ed *end of stream delimiter* (esd). Il preambolo è una sequenza alternata di uni e zeri per 8 sestetti che consente la sincronizzazione del ricevitore. Siccome la trasmissione simultanea sulle quattro coppie di una tale sequenza genererebbe un'elevata emissione elettromagnetica, la trasmissione sui canali 2 e 3 è sfasata nel tempo tramite l'introduzione di tre bit di "riempimento" (*start fill pattern*) prima del preambolo. Questi tre bit, di valore "101", fanno sì che quando su due coppie si trasmettono gli uni del preambolo, sulle altre due si trasmettano gli zeri, riducendo così le emissioni. Per fare in modo che la trasmissione su ciascun canale sia composta da un uguale numero intero di sestetti, dopo l'esd è aggiunto un *end fill pattern* di 3 o 6 bit in ciascun canale, in funzione del numero di quintetti di dato a partire dai quali è stata generata la sequenza.

Lo standard 802.12 prevede tre possibili soluzioni tecniche per il sottolivello *Physical Medium Dependent* (PMD), cioè per la trasmissione sul mezzo fisico dei quattro canali di dati.

La prima, 4-UTP PMD, associa ogni canale ad una coppia di un cavo UTP di categoria 3 o superiore (figura 11.18). Si tratta della tecnica principale di 100VG AnyLan che, come visto, ne ha determinato l'appellativo VG (Voice Grade). Lo standard introduce anche alcune specifiche sulla diafonia massima dei cavi a 25 coppie perché possano essere utilizzati da 100VG AnyLan. La trasmissione avviene con la codifica NRZ (paragrafo 3.1.2), e quindi la frequenza della fondamentale risulta di 15 MHz, soltanto il 50% in più di quella di Ethernet a 10 Mb/s.

La seconda e la terza soluzione, Dual Simplex STP PMD e Dual Simplex Fibre Optic PMD, prevedono l'utilizzo, rispettivamente, di un cavo a 2 coppie STP a 150 Ω e di una coppia di fibre ottiche. In entrambe si hanno a disposizione due soli canali trasmissivi, uno sempre in trasmissione e uno sempre in ricezione. Per trasmettere i quattro canali provenienti dal PMI è necessaria un'operazione di multiplexing, in cui si alterna la trasmissione dei sestetti provenienti dai quattro canali (figura 11.19), ottenendo un flusso di 120 Mb/s, anche in questo caso codificato in NRZ.

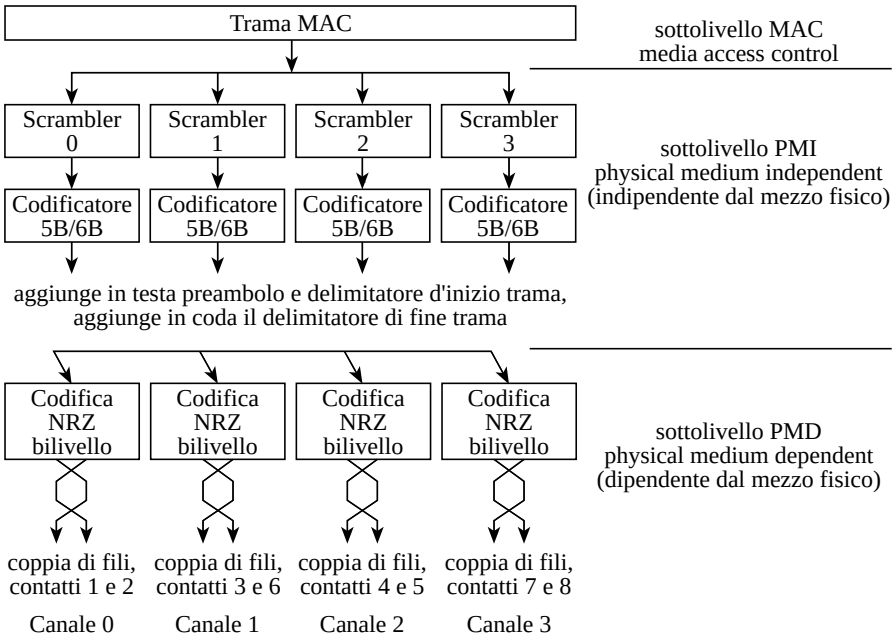


Fig. 11.18 - 100VG AnyLan: 4-UTP PMD.

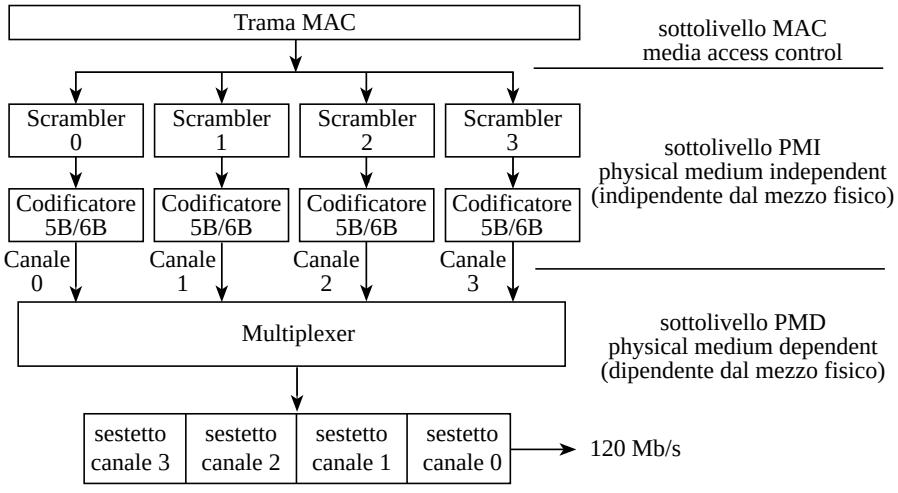


Fig. 11.19 - 100VG AnyLan: Dual Simplex PMD.

La figura 11.20 mostra come una rete 100VG AnyLAN su doppino a 4 coppie di categoria 3 usi la stessa piedinatura sul connettore RJ45 (1/2, 3/6, 4/5, 7/8) di Ethernet e Token Ring, conformemente agli standard EIA/TIA 568 e ISO/IEC 11801. Le informazioni di controllo dall'hub al nodo viaggiano sui canali 0 e 1, quelle dal nodo all'hub sui canali 2 e 3.

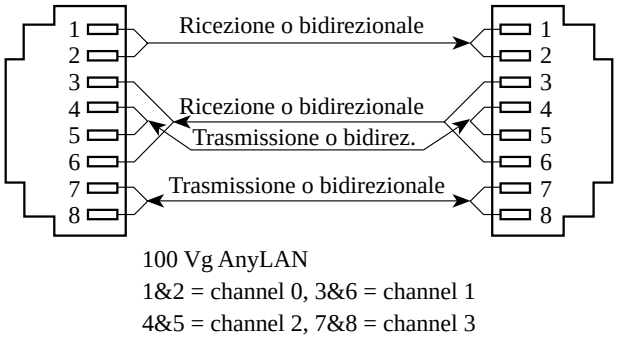


Fig. 11.20 - 100VG AnyLan: schema della configurazione delle coppie.

Il protocollo DPAM previsto dallo standard si basa su un meccanismo di richieste di trasmissione inoltrate dalle stazioni all'hub (o dagli hub) e su autorizzazioni a trasmettere concesse dall'hub ad una stazione alla volta. Per la gestione di tale protocollo sono definiti, nel sottolivello PMI, otto *Transmit Control State* (TCS) e otto *Receive Control State* (RCS). Tali stati assumono significati differenti a seconda che siano associati alle porte dedicate al collegamento in cascata degli hub, alle porte locali degli hub, oppure alle porte delle stazioni. I principali stati, necessari per comprendere il protocollo descritto più avanti, sono riportati in tabella 11.1. Si osservi l'utilizzo dei termini "up" e "down", intesi rispettivamente come trasmissione dalla stazione all'hub o da un hub ad un altro di livello superiore (up), e trasmissione da un hub alle stazioni o agli hub di livello inferiore (down).

Ciascun livello PMD (il 4-UTP e i due dual simplex) codifica tali stati con sequenze regolari di un pari numero di bit a zero e a uno che, una volta trasmesse, possono essere identificate semplicemente in base alla frequenza della fondamentale generata, un sottomultiplo della frequenza di bit (30 o 120 Mb/s). Per esempio, il dual simplex STP PMD codifica lo stato di Idle (001) ripetendo una sequenza di 26 uni e 26 zeri. Alla velocità di 120 Mb/s con codifica NRZ significa generare un ciclo della fondamentale ogni 52 bit, e quindi una frequenza pari a 120 : 52 = 2.30769 MHz. I due PMD dual simplex definiscono cinque frequenze diverse per codificare cinque degli otto stati previsti (due sono riservati e quindi non ancora utilizzati), mentre lo

stato di "pronto a ricevere" è codificato con il silenzio. Il 4-UTP PMD, invece, usa le quattro possibili combinazioni di due toni (anche in questo caso frequenze generate mediante sequenze regolari di bit) trasmessi contemporaneamente su due coppie, più il silenzio con cui codifica allo stesso modo i TCS 000 e 111.

Codice del Control State	Significato per il nodo quando riceve	Significato per l'hub quando riceve
000	Trasmissione disabilitata (pronto a ricevere)	Trasmissione disabilitata (pronto a ricevere)
001	Idle-Up	Idle-Down
010	Incoming Data Packet	Normal Priority Request
011	(reserved)	High Priority Request
100	Link Training Request-Up	Link Training Request-Down

Tab. 11.1 - 100VG AnyLan: principali stati di controllo.

Il significato degli stati di controllo è il seguente:

- *idle*: indica al nodo che l'hub non ha pacchetti in attesa e indica all'hub che non ci sono richieste pendenti;
- *incoming*: indica al nodo che un pacchetto può essere destinato alla sua porta; in questo modo (nel 4-UTP PMD) il nodo viene invitato a interrompere la trasmissione di toni di controllo sui canali 2 e 3 per prepararsi a ricevere il pacchetto;
- *normal priority request*: indica all'hub che il nodo sta richiedendo di trasmettere un pacchetto a priorità normale;
- *high priority request*: indica all'hub che il nodo sta richiedendo di trasmettere un pacchetto ad alta priorità;
- *link training request*: indica al nodo o all'hub che è richiesta l'inizializzazione del link.

Il link training è una procedura di inizializzazione del link in cui l'hub e il nodo si scambiano una serie di pacchetti speciali per eseguire un test funzionale dello stato del cablaggio e una verifica della possibilità di trasmissione senza errori. Inoltre, questa procedura permette all'hub di avere in modo automatico delle informazioni sul dispositivo connesso a ciascuna porta: infatti i pacchetti ricevuti dall'hub provenienti da un nodo che sta eseguendo il training contengono informazioni quali il tipo di dispositivo (concentratore, bridge, router, network test/

monitor equipment, etc.), il modo di funzionamento (normale o monitor), e l'indirizzo della stazione collegata a quella porta. Il link training è iniziato dal nodo quando questo e l'hub vengono accesi, o quando il nodo viene connesso per la prima volta all'hub. Se vengono riscontrate alcune condizioni di errore, può essere necessario che il nodo o l'hub richieda il training del link.

In figura 11.21 è illustrato un possibile schema di ricezione da parte di un end node e in figura 11.22 un possibile schema di trasmissione.

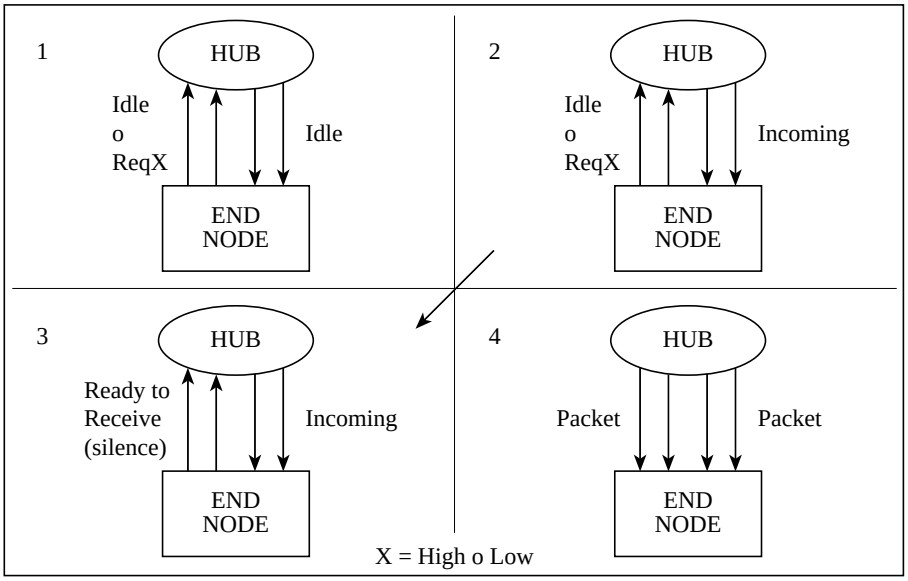


Fig. 11.21 - 100VG AnyLan: trasmissione da un hub verso un nodo.

Sfruttando la topologia a stella, 100VG AnyLAN usa l'intelligenza insita nell'hub per gestire al meglio l'utilizzazione e il controllo della rete. Questa intelligenza viene resa disponibile da una potente tecnologia frame switching chiamata Demand Priority: essa permette di minimizzare il ritardo della rete e, dato che lo schema di arbitraggio round-robin usato dal Demand Priority è completamente deterministico, di rendere deterministici la latenza massima e quindi il ritardo di un pacchetto.

Grazie al Demand Priority è possibile massimizzare il throughput della rete e ottenere un'efficienza media del 96% (95% con pacchetti di 1500 byte e 98% con quelli di 4500 byte) contro un massimo teorico del 70-80% che è tipico delle reti CSMA/CD.

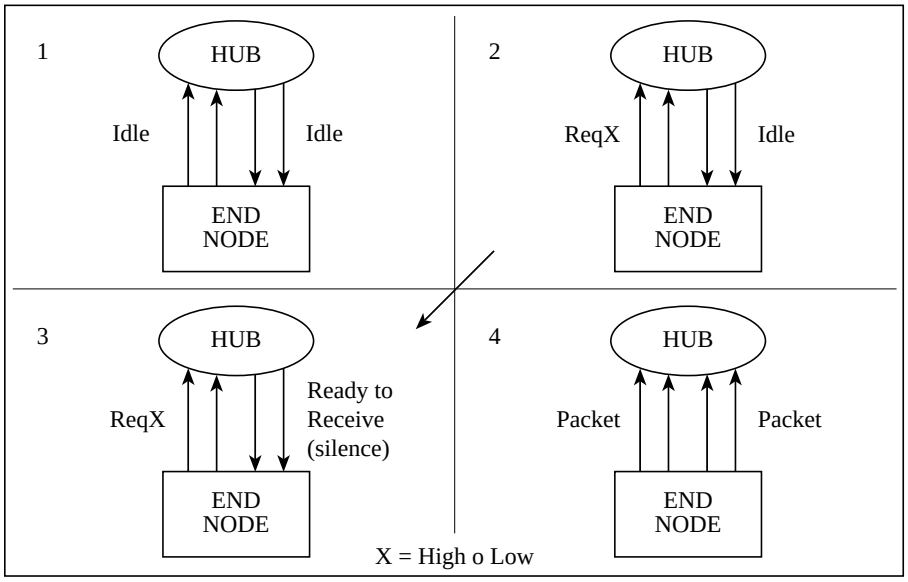


Fig. 11.22 - 100VG AnyLan: trasmissione da un nodo verso l'hub.

Inoltre, è possibile definire le porte degli hub in modo che vi vengano inoltrati soltanto i pacchetti broadcast ed i pacchetti multicast o unicast diretti alla stazione collegata. Questa funzionalità, se applicata a tutti gli hub della rete, fornisce un livello di Link Privacy superiore a quello normalmente ottenibile in altre reti. Per scopi di diagnosi, tuttavia, gli amministratori di rete possono attivare la ricezione di tutti i messaggi su singole porte per monitorare tutto il traffico dell'hub.

Demand Priority è un metodo di accesso al mezzo trasmissivo in cui i nodi avanzano una richiesta all'hub tutte le volte che devono inviare un pacchetto sulla rete. Ogni richiesta è caratterizzata da due possibili livelli di priorità: normale (per i normali pacchetti di dati) o alta (ad es., per i pacchetti contenenti dati di applicazioni multimediali). Alle richieste ad alta priorità viene garantito l'accesso alla rete prima di quelle a priorità normale, fornendo in questo modo un metodo appropriato per gestire le applicazioni "time-sensitive". Il livello di priorità dei pacchetti è stabilito dal software applicativo ed è passato come parte dell'informazione del pacchetto al sottostrato MAC.

La gestione delle richieste di trasmissione da parte dei nodi viene effettuata dagli hub mediante una procedura di arbitraggio *round-robin*: le porte vengono ciclicamente osservate secondo un ordine predefinito per individuare le richieste di trasmissione. Le richieste sono soddisfatte (cioè le porte sono abilitate alla

trasmissione di un pacchetto) nello stesso ordine, ma procedendo prima con quelle ad alta priorità, e poi con le altre.

Lo standard 802.12 prevede inoltre il collegamento ad albero degli hub, e quindi le richieste di trasmissione ad una porta di un hub possono provenire da una stazione oppure da un hub di livello inferiore. Nel caso si tratti di un hub, l'abilitazione a trasmettere ricevuta dall'hub di livello superiore attiva un ciclo di trasmissioni, abilitando in ordine tutte le porte con richieste pendenti alla priorità corrente. I nodi singoli quindi possono solo inviare un pacchetto alla volta, mentre un hub di livello inferiore con *n* nodi collegati potrà inviare fino a *n* pacchetti non appena selezionato durante il ciclo round-robin.

Ogni hub conserva due liste separate per le richieste a bassa e ad alta priorità. Le prime sono servite nell'ordine delle porte da cui provengono fin tanto che non arriva una richiesta ad alta priorità. In questo caso, dopo aver completato la trasmissione del pacchetto corrente, l'hub servirà la richiesta ad alta priorità. Prima che l'hub ritorni a servire la lista a priorità normale, saranno serviti tutti i pacchetti ad alta priorità. Per evitare la starvation delle richieste a bassa priorità durante un eccesso di traffico ad alta priorità, l'hub controlla continuamente i tempi di risposta alle request-to-send dei nodi. Se il ritardo supera un tempo massimo prestabilito, l'hub innalzerà automaticamente la priorità delle richieste da bassa ad alta.

In figura 11.23 viene esemplificato l'utilizzo del round-robin a due livelli di priorità: se, nell'istante t = 0, tutte le porte hanno richieste pendenti a bassa priorità, l'ordine di servizio dei pacchetti sarà: 1-1, 2-1, 2-3, 2-n, 1-3, 1-n. Se, invece, nell'istante t = 0 i nodi 1-1, 2-3 e 1-3 inviano una richiesta ad alta priorità, l'ordine di servizio dei pacchetti sarà: 1-1, 2-3, 1-3, 2-1, 2-n e 1-n. Si noti che ogni hub include una porta di uplink e *n* di downlink: la porta di uplink funziona come una normale porta, ma è riservata per connettere l'hub con un hub di livello superiore. Le *n* porte di downlink sono usate per connettere i nodi 100VG AnyLAN, siano essi stazioni o hub di livello inferiore. L'hub posto alla radice dell'albero prende il nome di *root hub*.

100VG AnyLAN permette il collegamento in cascata tra hub, anche con l'uso di vari mezzi trasmissivi, come evidenziato in figura 11.24. È ammessa la presenza di un massimo di 13 hub tra due stazioni (cioè fino a 7 livelli di profondità dell'albero). Se la rete ha solo il root hub la distanza massima tra due nodi è di 6 Km, ogni coppia di hub aggiuntiva riduce il diametro di 1100 m. Con 13 hub il diametro massimo è quindi 500 m.

Ovviamente, ogni singolo cavo è poi soggetto a limiti di lunghezza massima che dipendono dalla tipologia del cavo stesso.

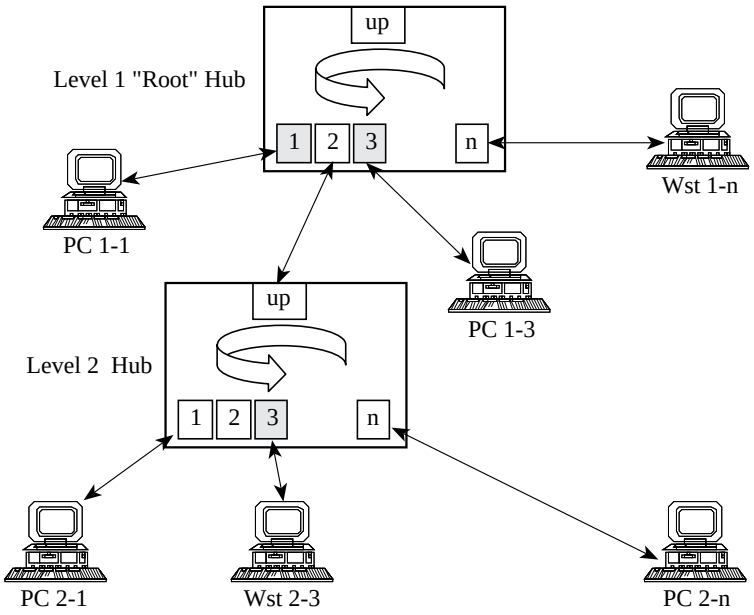


Fig. 11.23 - 100VG AnyLan: protocollo MAC.

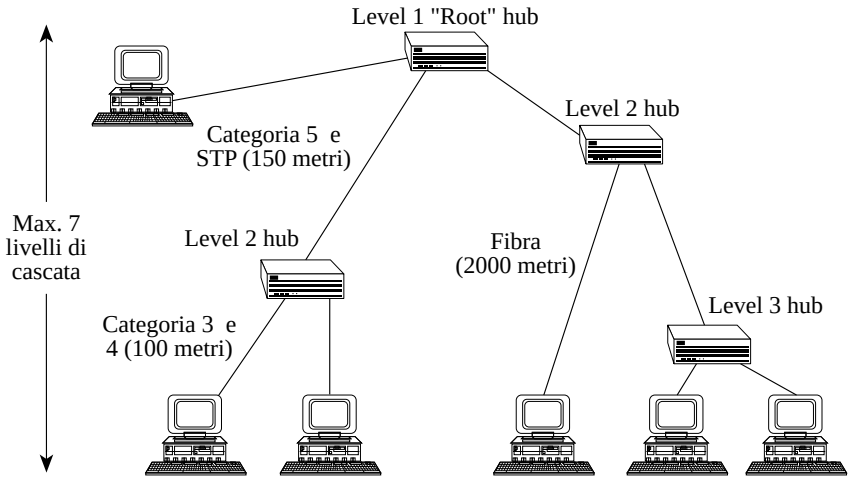


Fig. 11.24 - 100VG AnyLan: distanze e mezzi trasmissivi.

11.7 RETI WIRELESS

La rapida evoluzione della tecnologia di trasmissione "via etere" ha dato un nuovo impulso allo sviluppo dei sistemi *wireless* (senza fili), dettato anche dai diversi vantaggi che essi possono avere rispetto alle reti cablate: flessibilità nel posizionamento delle stazioni, facilità di installazione e riconfigurazione, possibilità di avere stazioni mobili.

Si cerca, quindi, di sviluppare sistemi con prestazioni analoghe alle reti *wired* (cablate) e con i vantaggi delle wireless, cercando di risolvere i problemi di efficienza, sicurezza e robustezza della trasmissione, che l'assenza del "filo" inevitabilmente porta.

Le reti wireless possono essere classificate in base alla copertura geografica e alla tecnologia su cui sono basate.

11.7.1 Classificazione in base alla copertura geografica

Le reti wireless possono operare in quattro distinti ambienti: *in-building*, *ambiente di campus*, *MAN*, *WAN*.

Quando la collocazione delle stazioni all'interno di un edificio varia molto raramente, si parla di ambiente *in-building tethered*. Questo segmento di mercato copre, ad esempio, i vecchi edifici dove è difficile o troppo costoso installare nuove reti cablate.

Nell'ambiente *in-building non-tethered*, invece, viene sfruttata la caratteristica di mobilità delle reti wireless. Si fornisce cioè una connessione tra un computer portatile e i servizi di una LAN, mentre l'utente si può spostare liberamente nell'edificio.

Si parla di ambiente di campus quando vi sono più edifici vicini compresi in un'area limitata. Anche in questo caso le reti wireless rispondono alle esigenze di connessione fra gli edifici e di mobilità delle singole stazioni all'interno del campus.

Per quel che riguarda le reti wireless a largo raggio (MAN e WAN) in grado di trasmettere dati in un'area metropolitana o in un'intera nazione, quelle attualmente in funzione sono caratterizzate da una velocità relativamente bassa (da 4.8 a 19.2 Kb/s). I principali tipi di reti wireless "wide-area" si basano sulle reti radio pubbliche e private a commutazione di pacchetto e sulle reti cellulari a commutazione di circuito.

11.7.2 Classificazione in base alla tecnologia usata

La scelta della tecnologia per la realizzazione di una rete wireless è ovviamente strettamente legata alla topologia e alla tipologia della rete stessa.

Attualmente le tecnologie wireless sono: *powerline*, *ottica*, *radiofrequenze*, *microonde*, *cellulare e satellitare*.

Powerline

La tecnologia "powerline" fa uso dei comuni fili della corrente all'interno di un edificio per trasmettere il segnale. In assenza di interruzioni (ad esempio trasformatori) nella rete elettrica, è possibile stabilire un link di comunicazione tra chiamante e ricevente mediante onde convogliate. A causa della gran quantità di rumore presente sui fili e del tipo di mezzo usato per trasmettere la corrente, la velocità di trasmissione è generalmente bassa, tra 1.2 e 38.4 Kb/s. Il pregio maggiore di questa tecnologia è che è relativamente economica.

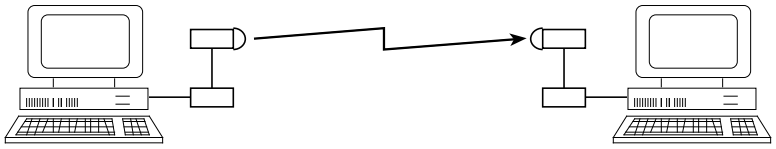
Ottica

La tecnologia ottica utilizza le lunghezze d'onda nell'infrarosso per trasmettere l'informazione. In una wireless LAN a raggi infrarossi (IR) ogni stazione è equipaggiata con un *transceiver* dotato per la trasmissione di un LED (*Light Emitting Diode)* che emette luce a raggi infrarossi e, per la ricezione, di un fotodiodo, operanti alla medesima lunghezza d'onda.

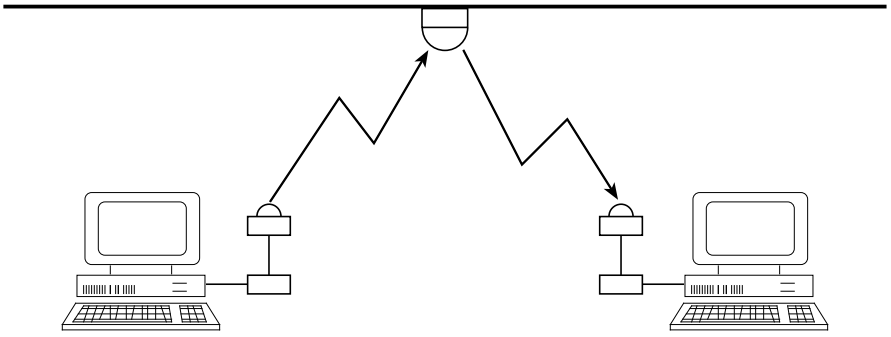
Si hanno a disposizione tre modi di radiazione degli IR per l'interscambio di dati tra le stazioni: *punto-punto*, *semi-diffusione* e *diffusione totale* (figura 11.25).

Nella modalità punto-punto, due transceiver devono essere perfettamente allineati per potersi illuminare reciprocamente con un fascio di luce IR. Lo scambio di dati tra le stazioni avviene modulando il fascio di infrarossi. Questa tecnica va bene per la realizzazione di LAN di tipo Token Ring, realizzando l'anello fisico mediante una sequenza circolare di link punto-punto. Con trasmissione laser-IR unidirezionale si possono coprire distanze anche di alcuni Km.

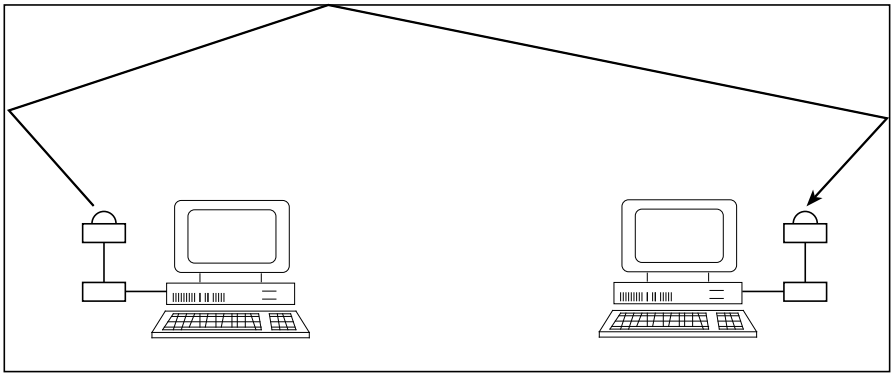
Nella modalità di radiazione per semi-diffusione, il segnale ottico emesso da una stazione viene captato da tutte le altre, realizzando così delle connessioni punto-multipunto o broadcast. Si sfrutta una superficie riflettente sulla quale vanno a collimare i fasci IR provenienti dai transceiver di tutte le stazioni: con questa configurazione, per il principio di diffusione della radiazione luminosa, il raggio proveniente da una stazione verrà riflesso verso tutte le altre rendendo così possibile una comunicazione di tipo broadcast.



a) Propagazione Punto-Punto



b) Propagazione per Semi-diffusione (con satellite)



c) Propagazione per diffusione totale

Fig. 11.25 - Modalità di radiazione dei raggi infrarossi.

La superficie riflettente può essere passiva, di solito il soffitto della stanza ove ha sede la LAN, oppure attiva, cioè realizzata mediante un dispositivo, detto *satellite*, che serve ad amplificare e rigenerare il segnale ottico prima di effettuarne il broadcast (funziona praticamente come un repeater). La diffusione passiva

richiede più potenza nei transceiver delle stazioni, ma consente una più facile installazione della rete dal momento che non occorre il posizionamento del satellite.

Nella radiazione per diffusione totale, la potenza ottica emessa da un transceiver deve essere tale da consentire al raggio di diffondersi per tutto il volume della stanza dopo una serie di riflessioni multiple sui muri. Questo segnale verrà captato da qualunque altra stazione all'interno dello stesso spazio, senza la necessità di alcun particolare orientamento di quest'ultima.

La presenza di riflessioni, tuttavia, limita la massima velocità di trasmissione a causa dell'interferenza dovuta al fenomeno del *multipath* (per cui un segnale può essere ricevuto attraverso più cammini caratterizzati da differenti ritardi).

Le modalità di radiazione per semi-diffusione e diffusione totale, dal momento che consentono una comunicazione broadcast, sono adatte all'implementazione di reti di tipo Ethernet. In particolare, la prima va bene per reti con stazioni fisse (tethered), la seconda permette la realizzazione di reti con stazioni mobili.

Le reti wireless ad IR possono essere installate solo nell'ambito di un'unica stanza, in quanto le stazioni devono trovarsi in linea ottica nel caso di link punto-punto, oppure avere una superficie riflettente comune, nel caso dei link punto-multipunto ottenuti per semi-diffusione, oppure ancora devono essere situate tutte nello stesso volume, se si usa la diffusione totale. È inoltre difficile garantire la compresenza di più network isolate poiché, anche se si possono utilizzare nella trasmissione diverse frequenze portanti, la possibilità di passare da una frequenza ottica ad un'altra è difficile e costosa da ottenere. Nonostante queste limitazioni, gli IR offrono notevoli vantaggi come, ad esempio, l'immunità alle interferenze elettromagnetiche (EMI), l'intrinseca sicurezza della trasmissione (perché in ambiente molto limitato) e l'assenza di licenze da parte delle PTT (in Italia, il Ministero delle Poste e Telecomunicazioni) per le installazioni.

La tecnologia dei raggi infrarossi è sicuramente la più matura tra quelle utilizzate nell'ambito delle reti wireless in quanto è da una ventina d'anni che la trasmissione dati mediante IR è realizzata mediante apparecchiature commerciali (si pensi alle calcolatrici HP degli anni '70).

Photonics e InfraLAN sono due fra le diverse aziende che costruiscono prodotti di networking basati su tecnologia IR.

Photonics presenta due serie di prodotti che utilizzano la trasmissione IR: *Collaborative* e *Cooperative*, destinati rispettivamente al mondo DOS/Windows e al mondo Macintosh. I due sistemi hanno in comune solo il transceiver ottico, dato che Cooperative lavora in modo nativo con il protocollo Localtalk, a 230 Kb/s, invece Collaborative lavora con trame Ethernet e metodo CSMA/CA, con velocità

di 1 Mb/s. I dati forniti da Photonics indicano che la copertura di un transceiver viene garantita all'interno di stanze di 10 m di lato.

InfraLAN produce un prodotto omonimo, una rete Token Ring composta da Multistation Access Unit (MAU). Ogni MAU supporta fino a sei dispositivi Token Ring. I MAU si attaccano a due transceiver che InfraLAN chiama "nodi ottici": questi nodi forniscono la connessione wireless attraverso cui passa il token. I nodi devono essere posizionati in modo tale che si possano vedere direttamente per comunicare. La velocità è paragonabile a quella di una rete Token Ring tradizionale e la distanza massima a cui possono essere posti i transceiver è circa 30 m.

Radiofrequenze (RF)

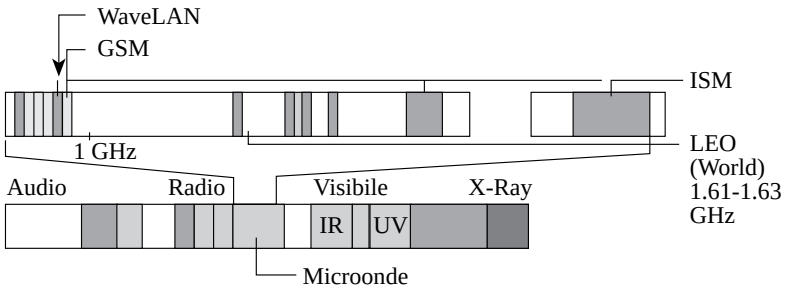
L'utilizzo delle radiofrequenze è ostacolato dal fatto che la complessità dei *radio-transceiver* cresce con il crescere della frequenza di trasmissione, e il costo è in generale più elevato del corrispettivo IR, anche se può essere in parte abbattuto sfruttando la componentistica ad alta diffusione (ad esempio la telefonia cellulare).

Uno dei vantaggi di questa tecnologia risiede nella possibilità di coprire aree estese, che superano i limiti di un singolo ambiente. Con una trasmissione a bassa potenza (<1W) si possono coprire distanze di circa 1 Km all'aperto e 50-100 m al chiuso, a seconda del numero di pareti da attraversare. Un ulteriore vantaggio della trasmissione RF consiste nella possibilità di permettere la compresenza di più network isolate, mediante la variazione della frequenza della portante trasmissiva.

La scelta delle frequenze e della modalità di trasmissione è strettamente legata alle esigenze di progetto e alla regolamentazione presente nei diversi Paesi.

Nel 1985 il Federal Communication Commitee (FCC) assegnò tre bande di frequenza, nel campo delle microonde, alle trasmissioni senza licenza con potenza massima di 1 W. Queste bande, 902 - 928 MHz, 2400 - 2483 MHz e 5725 - 5850 MHz, erano precedentemente disponibili per applicazioni Industriali, Scientifiche e Mediche, da ciò il nome *bande ISM* (figura 11.26).

Dal 1985, avendo a disposizione le bande ISM, alcuni costruttori di prodotti di networking iniziarono a progettare dei dispositivi per wireless LAN operanti a tali frequenze. Essendo bande piuttosto strette e, non necessitando di licenza, aperte a chiunque volesse utilizzarle (con il solo vincolo della potenza massima di 1 W), si arrivò ben presto ad un livello di interferenza inammissibile e ciò portò l'FCC a imporre l'utilizzo della tecnica di modulazione *Spread Spectrum* (SS) per la trasmissione in banda ISM.



Servizio	Frequenze
Radio AM	535-1605 KHz
Telefono Cordless	46-47 48-49 MHz
Radio FM	88-108 MHz
TV USA	54-88 174-216 470-806 MHz
ARDIS	855-865 MHz
Telefono Cellulare USA	826-849 860-894 MHz
Telefono Cellulare Europa	872-905 917-950 MHz
RAM (Mobitex)	896-902 MHz
NCR (WaveLAN)	902-928 MHz
GSM (Telefono Digitale)	890-915 935-960 MHz
LEO (satellite)	1.97-1.98 GHz
Banda ISM	902-928 2400-2480 5150-5250 MHz
California Microvawe	2.40-2.48 GHz
Forni a microonde	2.43-2.46 GHz
Motorola (Altair)	18.8-19.2 GHz

Fig. 11.26 - Utilizzo dello spettro elettromagnetico per le telecomunicazioni.

La tecnica di modulazione Spread Spectrum è nata alla fine della Seconda Guerra Mondiale per scopi militari: serviva per prevenire l'interferenza durante il controllo di armi telecomandate. Consiste nel distribuire l'energia di un segnale a banda limitata su di una banda molto più ampia al fine di abbassarne notevolmente la densità spettrale di energia. L'idea è quella di ottenere un segnale con un livello energetico al di sotto di quello del rumore ambientale, che, come è noto, è costante e a banda pressoché illimitata, per renderlo non intercettabile. In ambito civile lo scopo è quello di minimizzare le interferenze che inevitabilmente si hanno tra più segnali che condividono la stessa banda.

Esistono due tecniche per ottenere un segnale Spread Spectrum da uno a banda limitata:

- *Direct Sequence Spread Spectrum* (DSSS): il segnale trasmesso è modulato con una sequenza pseudo-casuale binaria (*chipping sequence*, figura 11.27). Per trasmettere un 1 si invia la sequenza di chipping affermata, per trasmettere uno zero la sequenza negata. La velocità relativa tra frequenza pseudo-casuale

e trasmissione (cioè la lunghezza della sequenza di chipping) è, nel caso commerciale, compresa tra 10 e 100, mentre in quello militare tra 1000 e 10000. Il ricevitore per ricostruire l'informazione esegue l'EXOR tra segnale e sequenza pseudo-casuale: se sono in fase, il risultato è il segnale trasmesso.
Mediante tale tecnica si trasmette ancora con una singola portante a frequenza fissa, come nelle trasmissioni tradizionali, ma, grazie alla sequenza di cipher e allo schema di modulazione usato, la potenza del segnale si distribuisce su uno spettro più ampio.

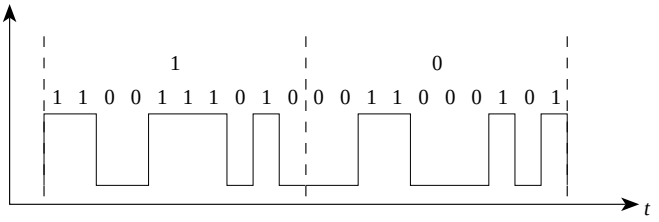


Fig. 11.27 - Esempio di trasmissione DSSS.

- *Frequency Hopping Spread Spectrum* (FHSS): tutta la banda disponibile è divisa in un insieme di canali di uguale larghezza. La trasmissione avviene per un certo periodo di tempo (*dwell time*) su un canale poi passa su un altro seguendo una precisa sequenza (*hopping sequence*, figura 11.28). Tale sequenza può essere predeterminata o trasmessa essa stessa insieme ai dati, comunque deve essere tale da garantire un ugual uso di tutti i canali di trasmissione. Quando il dwell time è minore del tempo di bit si parla di *fast-frequency hopping*, mentre quando il dwell time è (molto) maggiore del tempo di bit di parla di *slow-frequency hopping*. I sistemi basati sul primo tipo sono più costosi e ad alto consumo, ma, dal momento che ogni bit di dato viene trasmesso su molti canali, offrono il vantaggio di una maggiore tolleranza alla distorsione selettiva in frequenza. Lo slow-frequency hopping, invece, permette una maggiore facilità nel sincronismo dell'hop.

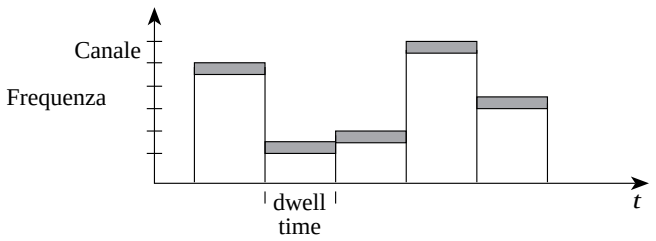


Fig. 11.28 - Esempio di trasmissione FHSS.

La scelta della banda in cui operare dipende dalle esigenze di lavoro. In tabella 11.2 è riportato un confronto fra le caratteristiche delle bande ISM. Attualmente la più utilizzata ed affollata è la prima (902-928 MHz), ma l'attenzione si sta spostando velocemente verso la seconda (2.4-2.483 GHz), che presenta vantaggi di ampiezza, di universalità (è utilizzabile senza licenza in tutto il mondo) e di costo (la componentistica può in parte sfruttare la tecnologia al silicio, di basso costo).

	I	II	III
Frequenze	902-928	2.4-2.4835	5.725-5.850
Larghezza di banda	26 MHz	83.5 MHz	125 MHz
Necessità di licenza FCC	No	No	No
Utilizzabilità	USA/Canada	Ovunque	USA/Canada
Costo tecnologia	Basso (Si)	Basso/medio (Si, GAAs)	Alto (GaAs)
Dimensione canali FH	0.5 MHz	1 MHz	1MHz
Numero canali FH (USA)	Elevato	Basso	Quasi nullo
Sorgenti di interferenza (USA)	Utilizzatori primari - molte LAN - molti non-Spread Spectrum	Utilizzatori primari - poche LAN - pochi non-SS - forni a microonde	Utilizzatori primari - pochissime LAN - pochissimi non-SS
Sorgenti di interferenza addizionali (nel mondo)	Telefoni cellulari		Alcuni radar

Tab. 11.2 - Confronto fra le bande ISM.

Il prodotto di networking più noto basato sulla tecnica di modulazione Spread Spectrum nella banda ISM 902-928 MHz è WaveLAN di NCR Corporation. Esso utilizza la tecnica di trasmissione direct sequence con sequenza di chipping di 11 bit. Consta di una scheda che, oltre alla circuiteria per l'implementazione di Ethernet, ospita un transceiver a microonde da collegare esternamente ad una piccola antenna delle dimensioni di un floppy disk da 5.25", che consente una portata di circa 250 m. Esiste anche un'antenna di dimensioni maggiori per portate fino a circa 3 Km. Il throughput dichiarato è di 2 Mb/s.

Xircom propone due prodotti wireless funzionanti a 2.4 GHz con SS frequency hopping: lo *Xircom credit card adapter* in versione PCMCIA 2.0 tipo II, oppure *lo Xircom pocket netwave adapter* per porta parallela. Inoltre fornisce anche un *punto d'accesso* (AP) per collegamento a Ethernet che permette di creare una rete "infrastructured" con raggio compreso tra i 40 e 60 m. La capacità trasmissiva massima è di 1 Mb/s, tuttavia, dato che un punto di accesso può governare

contemporaneamente diversi canali, il throughput complessivo di un gruppo di lavoro può essere di 10/15 Mb/s.

Anche IBM ha presentato una soluzione wireless basata su trasmissione FHSS a 2.4 GHz con adattatore di rete PCMCIA. La scheda è destinata all'uso su personal computer portatili. Il throughput è di 1 Mb/s, quadruplicabile attraverso una tecnologia di compressione dati. Per il collegamento alla rete cablata è prevista una scheda dalle prestazioni analoghe da inserirsi in un personal computer. Secondo i dati forniti da IBM, il sistema riesce a trasmettere in un'area con il raggio di circa 200 m in spazi aperti.

Microonde

Alcuni costruttori hanno realizzato dei dispositivi per wireless LAN operanti in bande a loro licenziate. Uno dei più importanti è Motorola, che ha introdotto il sistema Altair, una rete Ethernet a microonde operante a 10 Mb/s. Esso si compone di *Altair Plus II*, per applicazioni wireless in-bulding, e *Altair VistaPoint*, bridge wireless per collegare LAN distinte. Entrambi i prodotti sfruttano la speciale tecnologia in radiofrequenza di Motorola che funziona a 18 GHz a basso consumo. Inoltre, Altair Plus II offre capacità di network management con l'*Altair Extended MIB* (Management Information Base), che permette il pieno controllo remoto della rete (wireless e non) da una singola stazione. Il sistema Altair Plus II fornisce un throughput massimo di 5.7 Mb/s. L'Altair VistaPoint è un bridge wireless per collegare LAN cablate o wireless anche tra piani o edifici diversi purché non troppo distanti: permette la comunicazione di segmenti di LAN a una distanza di 15 m oppure, nella versione "long-range", fino a 1.2 Km negli USA e 2.1 Km nella maggior parte degli altri paesi. Entrambi i bridge VistaPoint offrono una capacità trasmissiva massima di 5.3 Mb/s.

In Europa è stata presentato da Olivetti Systems & Networks una wireless LAN basata sullo standard Digital European Cordless Telecommunications (DECT), analoga al sistema Altair: si tratta di un hub collegato in topologia stellare con dei satelliti mediante link a microonde in modulazione di frequenza. Le frequenze usate sono nell'intorno dei 18 GHz con potenze molto ridotte.

Cellulare

Dal momento che le frequenze trasmissive sono una risorsa limitata, è meglio riutilizzarle il più possibile. È questa la filosofia che sta alla base della tecnologia cellulare. In pratica si fa in modo che aree geografiche adiacenti (celle) usino insiemi di frequenze disgiunti. Le celle non adiacenti possono quindi riutilizzare le stesse frequenze senza interferenza.

Quando ci si sposta (*roaming*) da una cella ad un'altra, automaticamente, in modo trasparente, viene garantito il passaggio all'insieme di frequenze della nuova cella (funzione di *handover*).

Vi possono essere sistemi di trasmissione cellulare dedicati alla trasmissione dati oppure condivisi con la telefonia.

Un esempio di sistema misto è CDPD (*Cellular Digital Packet Data*), sviluppato da IBM, McCaw Cellular Data, Baby Bells ed altri. Esso permette di trasmettere pacchetti di dati saltando da un canale cellulare a un altro per sfruttare i vuoti in mezzo al traffico vocale. Infatti tutte le chiamate cellulari devono avere un periodo di silenzio di 5 ÷ 10 secondi dopo la sconnessione per il reset della linea stessa; in questo intervallo i dati possono essere inviati a una stazione di base e poi al ricevitore. CDPD offre velocità fino a 19.2 Kb/s.

Nel caso di trasferimenti di file lunghi può essere invece utile acquisire un canale cellulare fino al completamento della trasmissione: è questa la via seguita da CSC (*Circuit Switched Data*) di McCaw Cellular Communications.

In via di realizzazione sono i PCS o Personal Communication Services, una serie di servizi che andranno dalla telefonia a pagamento alle sofisticate PCN (Personal Communication Networks), nati non come alternativa ma per coesistere con i sistemi esistenti di tipo cellulare e cablato: le celle sono più piccole di quelle convenzionali e i trasmettitori sono meno potenti, ma offrono una banda maggiore. L'FCC, a seguito di una petizione avanzata da Apple Computer Inc., ha allocato 160 MHz per i PCS nella banda compresa tra 1.85 e 2.2 GHz, 40 MHz per gli utenti senza licenza e 120 MHz per i fornitori di servizi con licenza.

Satellitare

Le caratteristiche principali delle trasmissioni mediante satellite sono l'estensione della copertura geografica e il funzionamento intrinsecamente broadcast.

I satelliti sono classificati in tre grosse categorie: *geosincroni* (GEO), *big Low Earth Orbit* (big LEO*) e little Low Earth Orbit* (little LEO).

- I sistemi geosincroni includono Inmarsat e OmniTracs, ma essendo i satelliti a 36.000 Km di quota (unica altezza possibile per la geosincronicità) la potenza richiesta al trasmettitore per raggiungerli è troppo elevata per trasmettitori portatili;
- Proposte di "big" LEO includono Aries, Ellipso, Globalstar, Iridium e Odyssey. Ad esempio, *Iridium* di Motorola offrirà comunicazioni telefoniche cellulari mondiali da 77 satelliti collocati in sette orbite polari;
- I "little" LEO includono Leosat, Orbcomm, Starnet e Vitasat.

Negli USA la banda più popolare per la comunicazione satellitare è la "C band": 6 GHz per l'uplink (Terra-satellite) e 4 GHz per il downlink (satellite-Terra). I satelliti più nuovi operano nella "*Ku band*": 14 GHz per l'uplink e 12 GHz per il downlink.

La tabella 11.3 riassume le principali caratteristiche delle tecnologie analizzate.

Tipo di WLNA	Velocità	Estensione	Vantaggi	Svantaggi
Powerline	da 1.2 a 38,4 Kb/s	da 5 m ad alcuni Km	- Economicità	- Elevato rumore nella trasmissione
Infrarossi	da 230 Kb/s a 16 Mb/s	da 30 m a 200 m	- Flessibilità di installazione, riconfigurazione e manutenzione - Tecnologia consolidata e sicura - Velocità al pari delle reti cablate - Immunità alla interferenze EMI - Assenza di licenza FCC - Buona mobilità	- In alcune implementazioni è indispensabile il perfetto allineamento delle stazioni - LAN confinate in un unico volume - Problemi di interferenza con luce ambientale forte - Difficile comprensenza di network isolate
Radio-frequenza	2 Mb/s	da 250 m a 3 Km	- Flessibilità di installazione, riconfigurazione e manutenzione - Penetrazione dei muri portanti - Assenza di licenza FCC - Possibilità di compresenza di network isolate	- Suscettibilità alle interferenze EMI - Velocità ridotta rispetto alla LAN cabalte - Esposizione utenti a radiazioni elettromagnetiche - Scarsa mobilità
Microonde	10 Mb/s	80 m	- Flessibilità di installazione, riconfigurazione e manutenzione - Velocità al pari delle reti cablate - Immunità alle interferenze EMI	- Propagazione del segnale limitata - Esposizione utenti a radiazioni elettromagnetiche - Licenza FCC
Cellulare	fino a 19.2 Kb/s	Rete cellulare	- Uso della rete cellulare telefonica preesistente - Tecnologia ad alta diffusione	- Possibili interferenze in radiofrequenza - Ritardi elevati
Satellitare		Migliaia di Km	- Trasmissione broadcast - Ampia copertura del territorio	- Costi iniziali elevati

Tab. 11.3 - WLAN - Analisi comparata.

11.8 STANDARDIZZAZIONE DELLE WIRELESS LAN

Esistono molteplici organizzazioni che si stanno occupando dello sviluppo di standard sulle wireless LAN. Sono coinvolte in tali attività delle entità nazionali, continentali e mondiali. Quella che segue è una panoramica sui lavori svolti dai vari enti di standardizzazione.

11.8.1 A livello mondiale

Il Taskgroup 8/1 del *Comité Consultatif International des Radiocomunications* (CCIR), che è una parte dell'*International Communication Union* (ITU), è al lavoro su un progetto denominato *Future Public Land Mobile Telecommunication System* (FPLMTS), il cui scopo è di ottenere una distribuzione valida a livello mondiale delle frequenze per le comunicazioni numeriche radiomobili, sia per fonia sia per i dati, fino a 20 Mb/s.

Nel 1992, durante la Worldwide Administrative Radio Conference (WARC 92), sono state assegnate al progetto FPLMTS due bande di frequenza, 1885 - 2025 MHz e 2110 - 2200 MHz, ed è inoltre stata approvata una risoluzione che stabilisce le linee guida per l'implementazione di sistemi FPLMTS ed invita il CCITT ad implementare tale tecnologia sfruttando le reti attualmente esistenti.

11.8.2 Europa

Nel marzo del 1992, il *Technical Committee for Radio Equipment and Systems* (TC RES), una componente dell'*European Telecommunications Standard Institute* (ETSI), ha approvato la versione definitiva del *Digital European Cordless Telecommunications Standard* (DECT). Questo standard è mirato alla telefonia e supporta dieci canali multiplati in frequenza (FDM) sui quali sono instradati 12 canali bidirezionali multiplati nel tempo (TDM) da 32 Kb/s. I canali possono essere usati separatamente per veicolare il traffico vocale, oppure in modo combinato ottenendo un unico canale numerico avente una banda aggregata di 7.68 Mb/s.

Due sottocomitati tecnici dell'ETSI hanno inoltre cominciato a lavorare su progetti concernenti le wireless LAN:

- il comitato RES2 si occupa di uno standard per sistemi di medie prestazioni operanti nella banda ISM intorno ai 2.4 GHz con tecnica di modulazione Spread Spectrum;

- il comitato RES10 sta preparando invece uno standard per High Performance European Radio Local Area Network (HIPERLAN), una wireless LAN ad elevate prestazioni, tra i 10 ed i 20 Mb/s, operante in una banda di 150 MHz allocata nell'intorno dei 5.2 GHz.

11.8.3 Giappone

Il *Telecommunications Technology Group* (TTG), un comitato consultivo del *Ministry for Post and Telecommunications* (MPT), che si occupa della regolamentazione e dell'assegnazione delle frequenze, ha raccomandato l'utilizzo delle bande 1215 - 3400 MHz e 17.7 - 21.1 GHz per le applicazioni di tipo wireless LAN. Basandosi sugli orientamenti offerti dal TTG, il *Research and Development Center for Radio Systems* (RCR), un altro organismo del MPT, fra gli obiettivi del quale c'è lo studio delle architetture dei sistemi per le wireless LAN, nel maggio 1992 ha redatto una specifica per LAN a medie prestazioni operanti nella banda 2.4-2.5 GHz con modulazione Spread Spectrum. RCR è anche al lavoro su una specifica per LAN ad elevate prestazioni, 10 Mb/s, nella banda 18-19 GHz.

11.8.4 Stati Uniti

Negli Stati Uniti l'organizzazione che si occupa della standardizzazione delle wireless LAN è l'IEEE Working Group for wireless LAN, denominato IEEE 802.11. Al lavoro di questo gruppo è dedicato il paragrafo successivo.

11.9 IEEE 802.11: WIRELESS LAN

L'IEEE 802.11 è un gruppo di lavoro che si occupa della standardizzazione del livello MAC e del livello fisico delle reti locali wireless. Il "working group" è suddiviso in due sottogruppi principali: MAC-sub-group e PHY-sub-group. Quest'ultimo è a sua volta suddiviso in "ad hoc groups", ciascuno relativo ad una ben specifica tecnologia.

Nel novembre del 1994 è stata approvata la prima bozza dello standard, ma il completamento dei lavori non è previsto prima della fine del 1996.

Lo studio mira a sviluppare una specifica di Medium Access Control e di Physical Layer per connessioni wireless per stazioni fisse, portatili e in movimento

all'interno di un'area locale (In-Building o Campus) in grado di supportare velocità trasmissive multiple, scelte a seconda dello stato del mezzo e della capacità delle stazioni, e comunque superiori a 1 Mb/s. Uno degli scopi principali del MAC group è di fare in modo che un singolo MAC possa supportare più livelli PHY, anche se questi fanno uso di tecnologie diverse (figura 11.29).

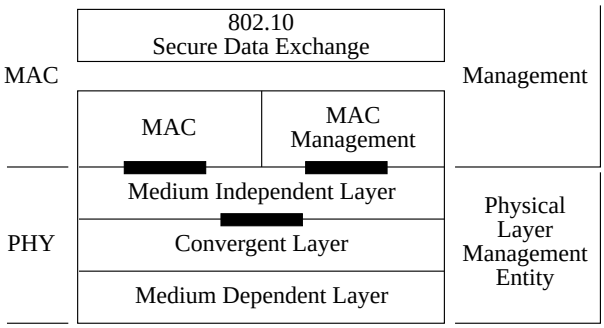


Fig. 11.29 - Visione globale dei livelli MAC e PHY dell'802.11.

Il wireless MAC supporta sia servizi connectionless a velocità comprese tra 1 e 20 Mb/s, sia servizi di tipo isocrono (*time bounded*) per controllo di processi, voce e video.

11.9.1 Livello Fisico

La convergenza tra MAC e lo specifico mezzo fisico è realizzata mediante la *Physical Layer Convergence Procedure* (PLCP). Essa si occupa di tradurre la MPDU (MAC Protocol Data Unit) nel formato opportuno per la trasmissione; ad esempio, inserisce all'inizio del frame il preambolo fisico occorrente.

Il sottolivello *Physical Medium Dependent* (PMD) realizza i meccanismi per l'individuazione del *clear channel* (mezzo trasmissivo libero), per la trasmissione e per la ricezione.

Già dal luglio 1992 il working group ha deciso di standardizzare tre tipi di trasmissione: infrarossi, radiofrequenza Frequency Hopping Spread Spectrum e radiofrequenza Direct Sequence Spread Spectrum. La prima in banda base, le altre nella seconda delle bande ISM (2.4-2.4835 GHz).

InfraRed PHY

L'InfraRed-PHY incluso nella bozza di Standard dell'802.11 è, come detto, in banda base. Il gruppo che si occupa della sua standardizzazione ha considerato la possibilità di aggiungere un IR-PHY di tipo *carrier-band*: mentre quello in banda base è adatto per piccoli dispositivi e per applicazioni a bassa velocità, quello in banda traslata sarebbe adatto per applicazioni ad alta velocità, dove dimensioni e consumi non sono importanti.

Per ora esiste solo la proposta in banda base per la quale sono previsti un *basic rate* a 1 Mb/s, che usa il 16-PPM (*Pulse Position Modulation*), e un *enhanced rate* a 2 Mb/s, che usa il 4-PPM.

Per quel che riguarda il formato del frame a livello PLCP viene aggiunto un preambolo (figura 11.30), con un campo (SYNC) per la sincronizzazione del ricevitore di lunghezza variabile da 57 a 73 *slot* temporali (*250 ns*) e con lo *start frame delimiter* (4 slot). Segue l'*header* con indicazioni sul *Data Rate* (DR), un campo della lunghezza di 32 slot (DCLA) per permettere al ricevitore di stabilire il livello DC, un campo indicante il numero di ottetti della MPDU ed infine il CRC. Gli ultimi due elementi dell'header, a differenza dei precedenti che hanno lunghezza temporale fissa, sono definiti in bit, quindi la loro trasmissione varia a seconda del data rate.

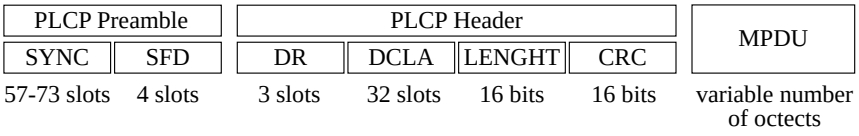


Fig. 11.30 - IR: PLCP Frame Format.

Per quanto riguarda la trasmissione, il picco di potenza ottica deve essere di 2W ± 20%.

Radiofrequenza DSSS PHY

Il PLCP Frame Format della trasmissione in radiofrequenza Direct Sequence Spread Spectrum prevede un preambolo costituito da 6 campi: 128 bit di sincronizzazione, 16 bit di *Unique Word* (o *Start Frame Delimiter*), 8 bit per indicare il *Data Rate* (ogni bit rappresenta 100 Kb/s), 8 bit riservati per usi futuri, 16 bit per indicare la lunghezza in ottetti della MPDU e, infine, 16 bit di CRC (figura 11.31).

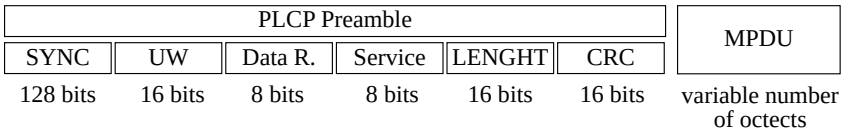


Fig. 11.31 - DSSS: PLCP Frame Format.

Per il DS-PHY sono specificati un *Basic Access Rate* di 1 Mb/s ottenuto con modulazione DBPSK (Differential Binary Phase Shift Keying) e un *enhanced access rate* di 2 Mb/s ottenuto con modulazione DQPSK (*Differential Quaternary Phase Shift Keying*). La sequenza di chipping è lunga 11 chip.

Come banda di trasmissione è stata scelta la banda ISM a 2.4 GHz in cui sono stati definiti 7 canali. Uno è specifico per il Giappone, mentre gli altri, per USA ed Europa, sono raggruppati in 3 coppie di canali, sebbene per l'Europa uno dei canali della prima coppia non possa essere utilizzato. I canali di una coppia possono operare senza interferenza. I canali di tutte e tre le coppie possono essere usati simultaneamente in un sistema tipo cellulare.

La potenza massima di trasmissione è fissata a 1 W in USA e 100 mW in Europa, mentre quella minima non deve essere inferiore ai 10 mW.

Radiofrequenza FHSS PHY

Il Frequency Hopping Spread Spectrum ha un data rate di 1 Mb/s con modulazione 2 level GFSK (*Gaussian Frequency Shift Keying*) e di 2 Mb/s con modulazione 4 level GFSK.

In USA e in Europa il range di frequenze utilizzabili, scelto sempre nella seconda banda ISM (2.4 GHz), va dai 2.402 GHz ai 2.482 GHz ed in esso sono individuati 79 canali per il frequency hopping di 1 MHz di ampiezza. La trasmissione deve essere tale da concentrare il 99% dell'energia all'interno del canale, ed avere la "20 dB bandwidth" inferiore a 1 MHz (figura 11.32).

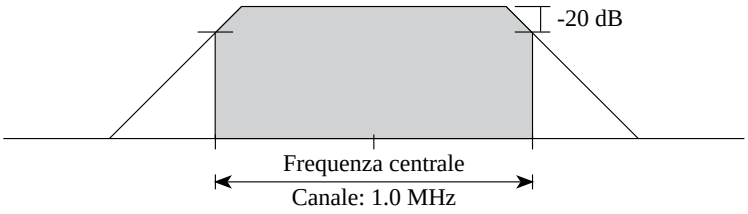


Fig. 11.32 - Occupazione della banda del singolo canale frequency hopping.

La sequenza di *hop* viene scelta in modo tale da poter collocare diverse reti simili nella stessa area geografica e per migliorare l'efficienza totale e il throughput di ciascuna rete. Sono definiti 3 insiemi di 22 sequenze di hop ciascuno, che rispettano il criterio di un solo canale adiacente che interferisce su ciascun lato del canale desiderato.

La frequenza dell'hop è controllata dai livelli superiori al PMD: dal momento che si deve poter massimizzare l'uso di ogni intervallo di hop e lo sfruttamento dell'intera banda di trasmissione, i livelli superiori devono dire al PMD quando saltare, definendo in questo modo l'hop rate del sistema. Questo preclude la nozione di un hop rate massimo. L'hop rate minimo, invece, è controllato dalle regolamentazioni ufficiali ed è definito dal numero di canali visitati diviso il tempo totale impiegato per completare la sequenza. Per gli USA, l'FCC stabilisce che un PMD deve visitare almeno 75 canali in un periodo di 30 secondi: 75/30 = 2.5 hop/s minimi.

A livello PLCP nel formato del frame viene aggiunto un *preamble* e un *header*. Il primo contiene 80 bit di sincronizzazione e 16 bit di Start Frame Delimiter. Il secondo è costituito da 3 campi: 6 bit di segnalazione per usi futuri, 10 bit di indicazione del numero di ottetti della MPDU e 16 bit di CRC (figura 11.33).

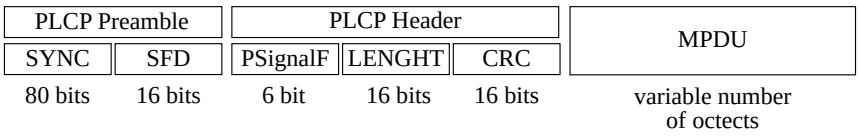


Fig. 11.33 - FHSS: PLCP Frame Format.

11.9.2 Livello MAC

Lo scopo del MAC group dell'IEEE 802.11 è quello di creare un singolo Medium Access Control per i diversi livelli fisici visti in precedenza.

Nasce così il wireless LAN MAC, che pone il suo fondamento nel DFWMAC (*Distributed Foundation Wireless MAC*), una proposta congiunta di NCR/Symbol e XIRCOM. Esso si presenta come supporto a due tipi di reti: *ad hoc LAN*, (piccola) rete di stazioni paritetiche, normalmente distribuite su una zona tale da permettere la trasmissione reciproca senza la presenza di una infrastruttura; *infrastructure network*, rete, anche vasta, caratterizzata dalla presenza di un *Distribution System*

(DS), a sua volta wireless o wired. Al distribution system si accede mediante stazioni apposite dette *Access Point* (AP, figura 11.34).

Ogni insieme di stazioni associate a formare un gruppo in cui comunicano direttamente fra di loro è detto *Basic Service Set* (BSS) caratterizzato da un identificatore, *BSS-ID*. L'insieme di più BSS, interconnessi mediante access point e un distribution system, forma un *Extended Service Set* (ESS), caratterizzato da un identificatore *ESS-ID*.

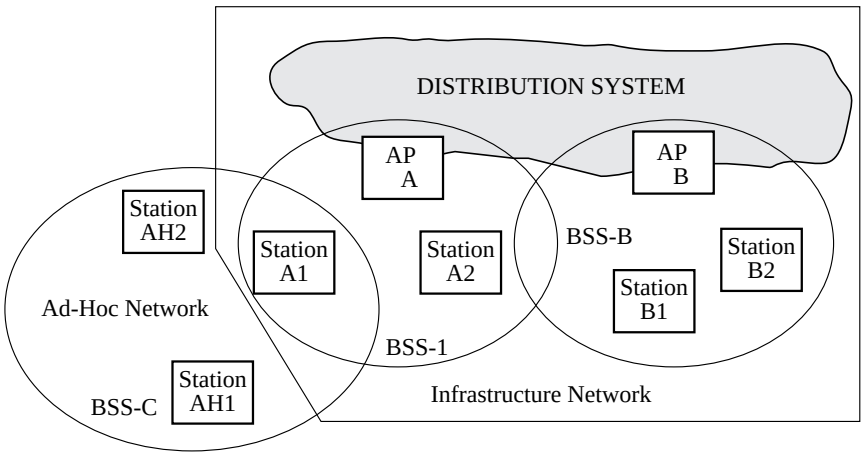


Fig. 11.34 - Rete *ad hoc* ed *infrastructure*.

Lo standard 802.11 specifica una serie di servizi propri di ciascuna stazione ed una serie di servizi propri del Distribution System. La tabella 11.4 llustra tali servizi.

Il principale metodo di accesso dell'802.11 MAC è una funzione di coordinamento distribuita (DCF): il C*arrier Sense Multiple Access with Collision Avoidance* (CSMA/CA). Esso è utilizzato per la trasmissione asincrona, e può essere affiancato da una funzione di coordinamento centralizzata (PCF) a maggior priorità per servizi time-bounded.

Categoria di servizi	Servizio	Scopo
Servizi forniti da ogni stazione	Autenticazione	Utilizzato per verificare l'identità delle stazioni che vogliono stabilire fra loro un link diretto di comunicazione. Non si tratta di autenticazione user-to-user o end-to end. L'802.11 fornisce il supporto e lascia la possibilità di implementare protocolli di autenticazione diversi.
	Associazione	Servizio mediante il quale una stazione entra a far parte di un BSS (deve essere preceduto dall'autenticazione). Nel caso di infrastructure network tale servizio è fornito unicamente dall'Access Point. In tale maniera il Distribution System sa a quale AP far riferimento per trasmettere un frame alla stazione.
	Disassociazione	Servizio mediante il quale si termina una precedente associazione. Non è una richiesta ma è una notifica, quindi non può essere rifiutata.
	Privacy	Utilizzato per stabilire un opportuno algoritmo per criptare i messaggi.
Servizi forniti dal Distribution System	Distribuzione	Servizio mediante il quale, utilizzando le informazioni di associazione, le MSDU vengono distribuite all'interno di un DS. Se ad es. la stazione A1 (figura 11.34) deve trasmettere un messaggio a B1, il percorso seguito è: da A1 all'AP-A, dall'AP-A al DS, dal DS all'AP-B, dall'AP-B a B1. L'AP che passa il messaggio dal BSS al DS viene detto "input AP". L'AP che passa il messaggio dal DS al BSS viene detto "output AP". Se A1 deve trasmettere ad A2, "input AP" e "output AP" coincidono e corrispondono ad A. L'802.11 non specifica la modalità di trasmissione nel DS.
	Integrazione	Permette lo scambio di MSDU tra DS ed una rete esistente. Viene svolto da una stazione particolare detta *portal*. L'802.11 non ne specifica l'implementazione.
	Riassociazione	Permette il trasferimento di una stazione da un BSS ad un altro (all'interno di un medesimo ESS), mediante il passaggio dall'associazione della stazione con l'AP del vecchio BSS a quella con l'AP del nuovo. Il servizio di riassociazione è quindi necessario per permettere la mobilità delle stazioni al di fuori del BSS.

Tab. 11.4 - Specifiche dei servizi.

11.9.3 MAC: Distributed Coordination Function

Il mezzo fisico wireless a differenza di quello wired non permette un facile Carrier Sense ed una facile Collision Detection. È possibile ad esempio che due stazioni facenti parte di una medesima infrastructure network riescano a comuni-

care con l'AP senza "sentirsi" fra di loro (problema del terminale nascosto). Il metodo di accesso scelto, il CSMA/CA, cerca una soluzione per tali problemi.

Una qualunque stazione che vuole trasmettere per prima cosa verifica se un'altra stazione sta trasmettendo (Carrier Sense), e se riconosce la presenza di trasmissioni si mette in attesa. Quando il mezzo si libera attende che rimanga tale per un intervallo di tempo minimo (*Distributed InterFrame Space:* DIFS), dopo di che inizia una fase di contesa per l'utilizzo del mezzo (*contention window*): la stazione sceglie un intervallo casuale (*backoff*) al termine del quale, se il mezzo è ancora libero, inizia la trasmissione. L'intervallo di backoff serve a ridurre la probabilità di collisione quando, alla fine di una trasmissione, ci sono molte stazioni in attesa che il mezzo si liberi.

L'intervallo di backoff è scelto tenendo conto di un parametro che oscilla tra un valore massimo ed uno minimo, raddoppiando ogni volta che si deve ripetere la trasmissione di un frame. In questo modo si allunga la finestra di contesa riducendo la probabilità di collisione nel caso di carico elevato della rete.

Quando una stazione, in attesa che termini l'intervallo di backoff, sente che il mezzo non è più libero, congela il tempo di backoff rimasto. Quando poi rileva il mezzo libero per un tempo pari ad un DIFS, non sceglie un nuovo intervallo di attesa, ma termina il precedente (figura 11.35). In questo modo si cerca di evitare la "starvation".

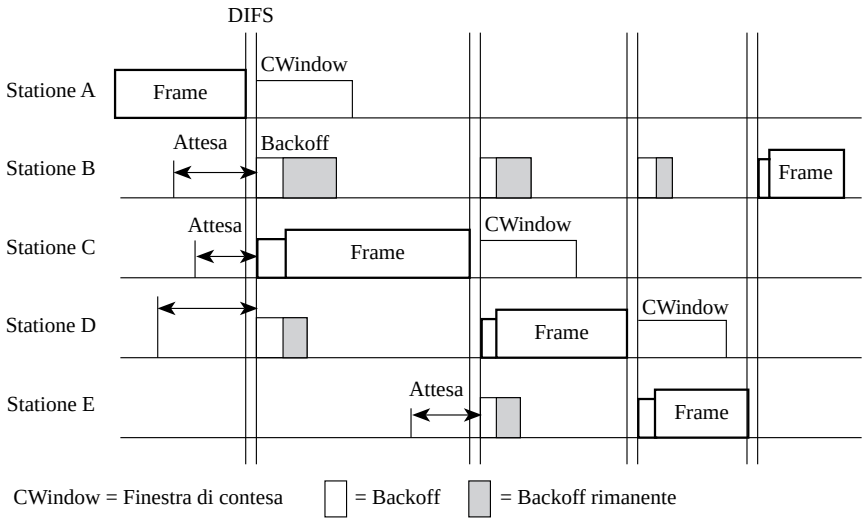


Fig. 11.35 - Procedura di backoff.

Comunque, il mecccanismo di backoff non esclude la possibilità di trasmissioni contemporanee, e quindi di collisioni. Per realizzare la "collision avoidance" lo standard prevede un protocollo *Request To Send* (RTS) - *Clear To Send* (CTS). Quando una stazione trova libero il mezzo allo scadere del tempo di backoff, non invia subito il dato, bensì un frame di RTS. Se riceve dal destinatario un frame di risposta CTS, allora procede all'invio del messaggio, altrimenti suppone che si sia verificata una collisione e si mette in attesa per riprovare.

Per evitare che durante i messaggi di protocollo si entri nuovamente in una contention window, il tempo di attesa per i messaggi di risposta e per l'invio dei dati dopo il CTS è più corto del DIFS; tale tempo è detto *Short InterFrame Space* (SIFS). La stazione destinataria, se la trasmissione ha successo, invia poi un messaggio di ACK. La figura 11.36 illustra la relazione tra DIFS e SIFS in corrispondenza di un ACK.

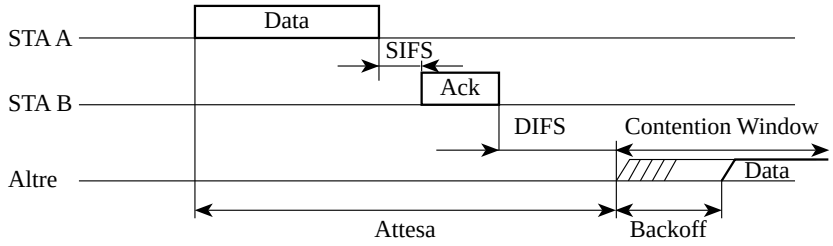


Fig. 11.36 - SIFS e DIFS in una trasmissione DATA-ACK.

Quando è in corso una trasmissione secondo il protocollo RTS/CTS, tutte le stazioni non interessate dovrebbero "sentire" il mezzo occupato. Tuttavia, a causa della bassa affidabilità della trasmissione, una stazione potrebbe non ricevere i messaggi e iniziare una trasmissione generando una collisione. Per prevenire questa eventualità, il protocollo realizza anche un "carrier sense virtuale". I messaggi RTS e CTS contengono informazioni sulla durata della trasmissione successiva, che le stazioni non interessate alla ricezione caricano in un registro detto *Net Allocation Vector* (NAV). Tale registro viene via via decrementato e ogni stazione ne attenderà l'azzeramento prima di cominciare la procedura di trasmissione (figura 11.37). Dal momento che il CTS è trasmesso dalla stazione di destinazione, le informazioni sulla durata della trasmissione raggiungono sia le stazioni vicine alla destinazione che quelle vicine alla sorgente.

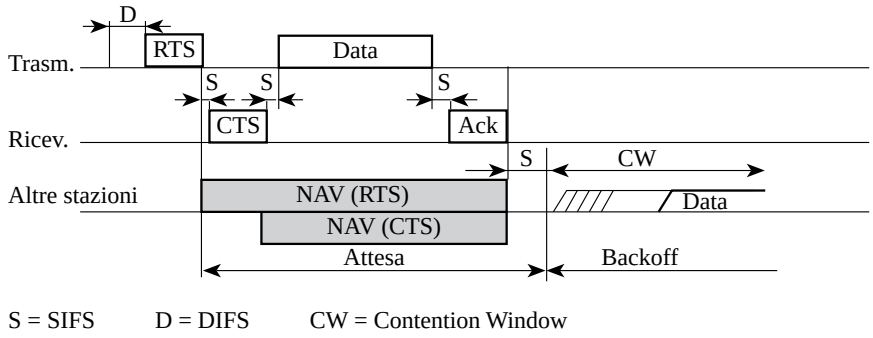


Fig. 11.37 - Net Allocation Vector (NAV).

L'utilizzo del protocollo RTS/CTS ha due controindicazioni: innanzi tutto, se il pacchetto di dati è corto, l'overhead introdotto può essere eccessivo; inoltre, non è applicabile nel caso dei pacchetti multicast e broadcast (in quanto più di una stazione potrebbe rispondere al RTS). Esiste pertanto la possibilità (obbligatoria per pacchetti al di sotto di una certa dimensione definibile a priori) di effettuare la trasmissione dei dati immediatamente allo scadere del tempo di backoff, se il mezzo è ancora libero. In questo caso è naturalmente possibile che una collisione impedisca la corretta trasmissione dei dati. Nel caso di pacchetti singlecast un messaggio di ACK segnala al mittente l'avvenuta ricezione, mentre per i pacchetti multicast e broadcast non c'è modo di sapere se la trasmissione è andata a buon fine.

Se la stazione trasmittente non riceve l'acknowledge entro un tempo limite, ritrasmette il frame dopo aver partecipato nuovamente alla contesa del mezzo. La mancata ricezione dell'acknowledge, tuttavia, non esclude che il frame di dati sia in realtà arrivato correttamente. Pertanto, ogni frame ritrasmesso ha un opportuno bit (*retry bit*) settato. L'eventuale ricezione di frame duplicati viene controllata mediante il confronto dell'MPDU ID, un campo di 16 bit ottenuto con funzione di hash dal *network identifier* (2 ottetti), dal *source address* (6 ottetti) e dal *sequence number* (1 ottetto). Ogni stazione mantiene l'MPDU ID degli ultimi frame ricevuti. Viene scartato il frame con il retry bit settato e MPDU ID uguale ad uno dei precedenti.

11.9.4 MAC: Point Coordination Function

Il wireless MAC di 802.11 prevede anche una funzione di coordinamento centralizzata (PCF: *Point Coordination Function*). Essa può essere gestita solo da alcune stazioni (*Point Coordination*), come ad esempio gli AP delle reti

infrastructure. Una PCF non è in grado di sovrapporsi con un'altra PCF sul medesimo canale trasmissivo.

La PCF usa una struttura a S*uperframe* (SF), dove si alternano il periodo di contesa, in cui è attiva la DCF, e il periodo senza contesa (*contention free*), in cui è attiva la PCF (figura 11.38). La lunghezza del Superframe è un parametro che può dipendere dai servizi supportati e dal livello fisico; nel caso di frequency hopping, ad esempio, deve essere un sottomultiplo intero del dwell time. La massima durata del periodo contention free è pari alla lunghezza del Superframe meno la lunghezza minima del contention period, che è pari a quella massima di un frame.

La PCF coesiste con la DCF disabilitandola temporaneamente grazie ad una scelta opportuna dei tempi per cui si deve attendere che il mezzo sia libero per poter trasmettere.

Il point coordinator (PC) dà inizio al periodo di trasmissione senza contesa. Il traffico diretto dal PC ad una stazione associata viene detto *CF-Down* mentre il traffico in direzione opposta viene detto *CF-Up*. Il PC diventa padrone del mezzo trasmissivo mediante un accesso prioritario. Infatti, all'inizio del Superframe, prima di iniziare una trasmissione CF-Down, attende che il mezzo sia libero per un periodo pari a un *Point InterFrame Space* (*PIFS*), più grande di un Short IFS ma minore del Distributed IFS. In tale maniera anticipa la normale trasmissione delle stazioni.

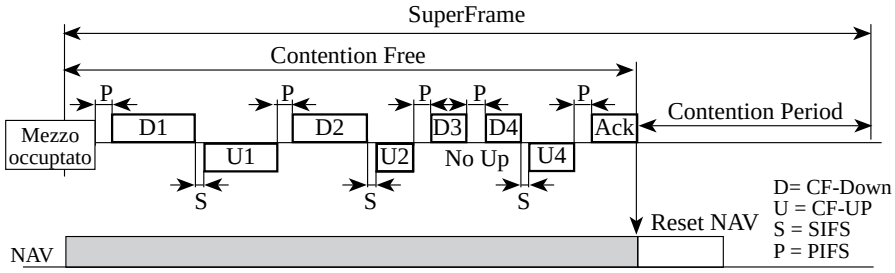


Fig. 11.38 - Struttura a Superframe e protocollo PCF.

Il PC coordina l'accesso al mezzo mediante il *polling*, mantenendo una tabella di quante stazioni ad esso associate hanno fatto richiesta del servizio contention free. Per ognuna di esse esegue un poll ed attende la trasmissione, che deve avvenire dopo un Short IFS altrimenti esegue il poll di un'altra stazione. Quando una stazione non trasmette per un lungo periodo viene cancellata dalla polling list.

Nel periodo contention free non vi sono frame di acknowledge. L'acknowledge è trasmesso settando un bit opportuno nel frame successivo. Ad esempio in figura 11.38 U1 contiene l'ack per D1 e così via.

Per diminuire il rischio di collisione, ad ogni inizio di Superframe ogni stazione carica nel Net Allocation Vector la lunghezza massima del periodo Contention Free. Al termine di questo il Point Coordination resetta il NAV di tutte le stazioni con la trasmissione di un frame opportuno.

11.9.5 MAC: sincronizzazione e power management

È importante che le stazioni di un medesimo BSS siano sincronizzate per permettere operazioni di *power management*, temporizzazione del Superframe, sincronizzazione nel frequency hopping.

Ogni stazione ha un timer interno che conta in microsecondi con modulo pari al valore del parametro TSFTIMERMOD; il timer delle stazioni di uno stesso BSS viene mantenuto sincronizzato mediante la *Time Synchronization Function* (TSF).

Questo non è in contrasto con il metodo di accesso CSMA in quanto non si tratta di protocollo sincrono. La temporizzazione di determinati eventi non implica, in questo caso, lo stabilire il tempo preciso in cui essi avvengono, ma il tempo minimo, in quanto ci possono essere dei ritardi.

Nel caso di reti infrastructure l'Access Point è il *timing master*. Esso invia periodicamente un frame opportuno di sincronizzazione, detto *beacon*. Ogni beacon contiene, oltre all'ESS-ID e al BSS-ID, il *timestamp* (31 bit) dell'AP all'esatto momento dell'inizio della trasmissione, e la lunghezza dell'intervallo tra due beacon (24 bit). Tale intervallo è fisso, ossia non è misurato relativamente alla trasmissione del beacon precedente: se la trasmissione di un beacon è ritardata perchè il mezzo è occupato, quelli successivi non ne risentono (figura 11.39).

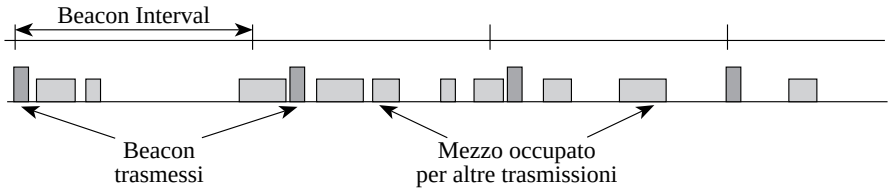


Fig. 11.39 - Trasmissione di beacon.

Ogni stazione che riceve un beacon assume come proprio il valore del timer dell'AP.

Nel caso di reti "ad hoc", le stazioni di un medesimo BSS che sono sincronizzate hanno un opportuno flag settato. Ogni stazione sincronizzata concorre alla trasmissione dei beacon periodici. La procedura seguita è simile a quella di

backoff: in pratica il beacon viene trasmesso dalla stazione che ha scelto casualmente l'intervallo di attesa di trasmissione più breve.

Nel beacon, oltre al timestamp della stazione trasmittente e alla lunghezza del beacon interval, è contenuto un campo indicante il "peso" della stazione (*weight*). Hanno peso maggiore le stazioni che fanno parte da più tempo del BSS, e sono in grado di sentire un maggior numero di stazioni. Quando una stazione non ancora sincronizzata riceve un beacon, si sincronizza copiando il timestamp. Invece quando una stazione già sincronizzata riceve un beacon calcola la differenza tra il timestamp e il proprio timer. Se è maggiore di una certa soglia allora vuol dire che all'interno del BSS si sono formati due gruppi sincronizzati diversamente ed è, quindi, necessario iniziare una opportuna procedura di riunificazione; altrimenti aggiusta il proprio timer di più o di meno a seconda del peso della stazione che ha trasmesso il beacon.

Una stazione che vuole entrare a far parte di un certo BSS deve sintonizzarsi sul canale opportuno e sincronizzarsi con le altre stazioni appartenenti a quel BSS. Questo è ottenuto mediante lo *scanning* di tutti i canali per un certo periodo di tempo fino a quando non vengono ricevuti messaggi da parte dell'AP o delle altre stazioni.

Sono possibili due tipi di scanning: *passive scanning* e *active scanning*.

Nel passive scanning le reti vengono individuate semplicemente mediante l'ascolto. La stazione scandisce tutti i diversi canali rimanendo in ascolto un certo periodo di tempo in ciascuno di essi, in attesa di un beacon. Nel beacon sono contenute le informazioni di BSS-ID e *timestamp* necessarie alla sincronizzazione. Questo metodo di scanning è efficiente se il BEACON_INTERVAL è relativamente breve e il PHY supporta pochi canali di trasmissione.

Nell'active scanning la stazione manda una *probe request*, cioè un frame broadcast contenente l'identificatore della rete cercata, ossia l'ESS-ID e uno specifico o un qualunque BSS-ID. Rimane poi in attesa per un certo periodo di tempo di un *probe response*. Se non ha avuto risposta passa al canale successivo e così via. È possibile che in un canale siano ricevuti più probe response.

Nel caso delle reti infrastructure, è l'AP incaricato di rispondere al probe request. Se su un medesimo canale sono in ascolto più AP interessati alla richiesta, tutti manderanno il proprio probe response (figura 11.40).

Nel caso di reti "ad hoc" ci si comporta come nella trasmissione del beacon: una sola stazione manderà il probe response.

Particolarmente curato nel wireless MAC è l'aspetto rigurdante il *power management*: è importante che in una rete wireless, dove molte stazioni possono consistere in computer portatili, i consumi possano essere ridotti. L'idea è quella di permettere di spegnere i transceiver il più a lungo possibile, bufferizzando i frame prima di trasmetterli e avvisando la stazione ricevente della presenza di

traffico in attesa mediante brevi messaggi periodici (*Traffic Indication Map: TIM*). Ai ricevitori è sufficiente ascoltare i TIM fino a che non viene annunciata una trasmissione a loro indirizzata.

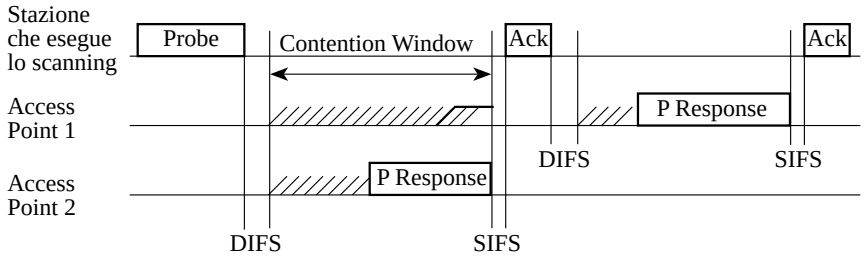


Fig. 11.40 - Active Scanning.

I transceiver delle stazioni possono essere in tre stati differenti: *transmit* (in trasmissione), *awake* (ricevitore in attesa), *doze* (trasmettitore e ricevitore spenti: consumo minimo). Il passaggio tra tali stati è regolato in maniera differente a seconda della modalità di power management scelta dalla stazione.

Nel caso di reti infrastructure particolari funzioni di power management sono svolte dall'AP. Esso mantiene lo stato delle stazioni ad esso associate, invia i TIM e bufferizza i frame diretti alle stazioni in power-save mode, o tutti i frame broadcast e multicast nel caso in cui nel BSS vi siano stazioni in power save mode.

Le stazioni possono essere in quattro *power management mode*:

- *CAM (Continuous Active Mode)*: transceiver sempre attivo; la stazione può trasmettere e ricevere in ogni momento.
- *TAM (Temporary Active Mode)*: come CAM solo per certi periodi.
- *PSP (Power Save Polling)*: la stazione ascolta i TIM, se vi è indicazione di traffico ad essa indirizzato esegue il polling dell'AP per ricevere i frame. Non è necessario che ascolti tutti i TIM.
- *PSNP (Power Save Non Polling)*: la stazione ascolta TIM particolari detti *Delivery TIM*, a seguito dei quali l'AP trasmette tutti i frame diretti alle stazioni PSNP senza bisogno del polling. È quindi necessario che la stazione ascolti tutti i TIM.

I TIM vengono trasmessi ad interavalli fissi in maniera che sia sufficiente alle stazioni in power save mode di passare solo periodicamente dallo stato doze a quello awake (figura 11.41). I TIM sono trasmessi ogni 20-50 ms, mentre i DTIM ogni 50-200 ms.

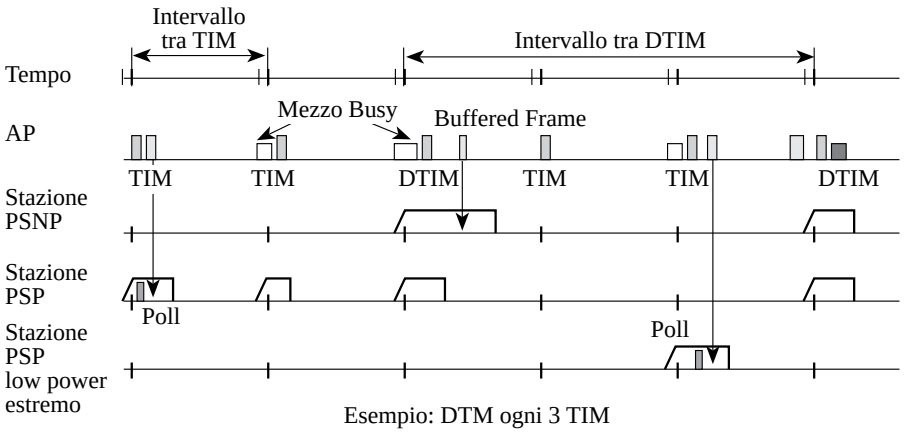


Fig. 11.41 - Power management in una rete infrastructure.

I frame broadcast e multicast sono trasmessi dall'AP immediatamente dopo aver avvisato le stazioni nei DTIM. Se una stazione non vuole perdere la trasmissione broad/multicast è necessario che ascolti tutti i DTIM.

Nel caso di reti "ad hoc" sono possibili solo il Continuous Active Mode e il Power Save Non Polling. Ogni stazione monitorizza lo stato delle altre stazioni. Quando una stazione deve trasmettere ad un'altra in power save mode, la avvisa mediante un *"ad hoc" TIM*. Gli "ad hoc" TIM vengono trasmessi in un intervallo detto *wake-up window*, in cui tutte le stazioni sono *awake*. La wake-up window si ripete ogni intervallo di beacon (figura 11.42).

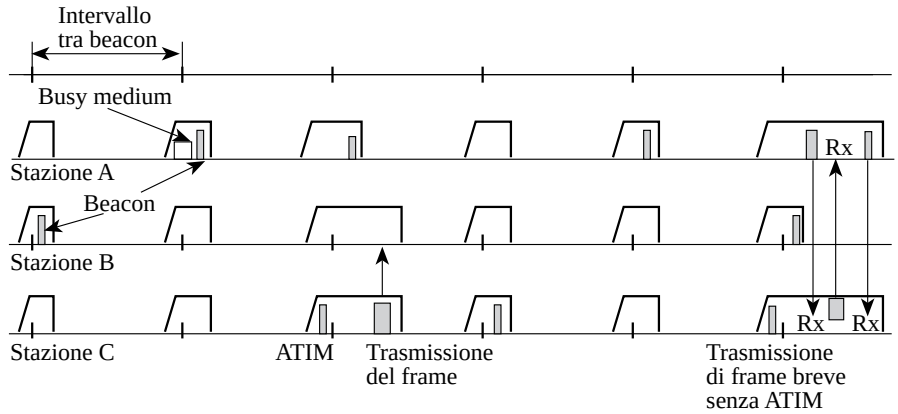


Fig. 11.42 - Power Management in una rete "ad hoc".

BIBLIOGRAFIA

[1] D. Cunningham, M. Spratt, S.Panditi, P.Colon, "Souped-up Ethernet", session at Interop 93, Parigi (F), October 1993.

[2] Chipcom, "Online Ethernet Interconnection Module", doc. nun. 17-00323-1, "StarBridge Turbo Switch", doc. num. 29-00138, "Galactica Network Switching Hub", doc. num. 29-00137, Chipcom Corp., Southborough MA (USA), 1993.

[3] SynOptics, "Ethernet solutions", P/N BR505-334US-A, "Product overview", P/N BR505-240US-C, SynOptics Communications Inc., Santa Clara, CA (USA), 1993.

[4] Fibronix, " FX 8610 Worksation Server operation manual", Fibronix International Inc. Hyannis MA (USA), October 1991.

[5] Nicolas Baran, "Wireless Networking", BYTE, Vol 17, No 4, April 1992.

[6] John P. Mello Jr. and Peter Wayner, "Wireless Mobile Communications", BYTE, Vol 18 No 2, February 1993.

[7] Peter Wayner, "Stretching the Ether", BYTE, Vol 18, No 2, February 1993.

[8] Angela Gunn, "Connecting over the Airwaves", PC Magazine, Vol 12, No 14, August 1993.

[9] Gary Berline and Ed Perratore, "Wireless LANs", PC Magazine, Vol 11, No 3, February 11 1992.

[10] Victor Hayes, "Radio-LAN Standardization Efforts", IEEE Proc. on Wireless LAN Implementation, September 17 - 18 1992.

[11] David F. Bantz and Frédéric J. Bauchot, "Wireless LAN Design Alternatives", IEEE Network, March/April 1994.

[12] Draft Standard IEEE 802.10.

[13] P802.11 Draft 20b3, November 1994, DS2972, "Wireless LAN Medium Access Control (MAC) and Physical Specifications".

[14] P802.12, D7, December 1994, DS4051, "IEEE Draft Standard for Demand-Priority Access Method, Physical Layer and Repeater Specifications for 100 Mb/s Operation".

[15] P802.3u/D2, July 1994, DS04127, "MAC Parameters, Physical Layer, Medium Attachment Units and Repeater for 100 Mb/s Operation (version 1.0)".

12

IL LIVELLO FISICO NELL'ACCESSO ALLE RETI PUBBLICHE

12.1 INTRODUZIONE

I servizi di trasmissione dati tra sedi separate da suolo pubblico sono in generale forniti dalle stesse aziende pubbliche o private detentrici del monopolio o delle concessioni governative per la telefonia. La principale ragione è dovuta al fatto che spesso vengono utilizzati gli stessi mezzi e canali trasmissivi già posati e disponibili per il servizio telefonico.

Il primo e più semplice servizio di trasmissione dati è infatti quello ottenibile attraverso un comune canale telefonico. Un apparecchio detto *modem* provvede a convertire i dati digitali provenienti dal computer o dal terminale e a trasformarli in modo da essere adatti per la trasmissione attraverso il canale telefonico, progettato per la trasmissione della voce. Un altro modem, all'altro capo del collegamento, opera la conversione inversa. Le comuni linee telefoniche sono dette "commutate", in quanto tramite i circuiti di commutazione nelle centrali possono essere collegate ad una qualsiasi altra linea, e quindi ad un qualsiasi utente, della rete. Proprio questa flessibilità rende questo tipo di collegamento dati ancora oggi estremamente importante e diffuso, anche grazie alla continua evoluzione tecnologica dei modem.

Per il collegamento stabile dei centri di calcolo, per esempio per la realizzazione di una WAN, l'impiego di linee commutate non è soddisfacente per diverse ragioni: tipo di tariffazione e quindi costo, bassa velocità e scarsa affidabilità. Per questo le compagnie telefoniche hanno messo a disposizione un diverso servizio: la *linea dedicata*, definita dalla Telecom Italia CDA (*Canale Diretto Analogico*). Si tratta di un collegamento fisso tra due sedi, con tariffazione su base annua, il cui tipo più comune consiste in un normale canale telefonico con l'eccezione che non attraversa i circuiti di commutazione delle centrali.

Con l'introduzione delle centrali numeriche i collegamenti analogici tra le centrali stesse sono stati rimpiazzati da dorsali digitali ad alta velocità. È stato così possibile da parte delle aziende telefoniche fornire una versione più evoluta del CDA: il CDN (*Canale Diretto Numerico*). Prolungando un collegamento digitale dall'interno della centrale fino alla presa dell'utente, è stato possibile fornire un servizio completamente digitale, a velocità più elevata e minor tasso d'errore.

Resta ancora analogico il servizio commutato, ma esistono già uno standard ed un servizio per una vera rete pubblica commutata digitale: ISDN (*Integrated Services Digital Network*). Con ISDN anche l'ultimo tratto di collegamento, dall'utente alla centrale, diventa digitale, consentendo l'integrazione di servizi diversi: telefonia, trasmissione dati, fax ad alta velocità, videoconferenza, teleallarmi, ecc.

12.2 INTERFACCE SERIALI

Tutte le apparecchiature di collegamento a linee di trasmissione dati analogiche o digitali prevedono la connessione del terminale, del computer o dell'apparecchiatura di rete (ad esempio router o bridge) mediante un'interfaccia seriale. Per convenzione, si denota DTE (*Data Terminal Equipment*) il terminale, il personal computer o la scheda di interfaccia di un mainframe, mentre le apparecchiature di comunicazione, quali i modem, vengono dette DCE (*Data Communication Equipment*).

Il collegamento tra DCE e DTE rappresenta una parte del livello Fisico del modello OSI. Esistono numerosi standard che definiscono caratteristiche elettriche e meccaniche dei cavi e dei connettori, codifica elettrica dei bit, ecc., tra cui RS-232, RS-449, V.24, V.35. Essi verranno discussi nella seconda parte di questo paragrafo. Prima, è necessario affrontare alcuni concetti generali sulle caratteristiche di questo tipo di collegamento. La trasmissione dei dati, che sono normalmente organizzati in byte, può infatti avvenire tra DTE e DCE in diversi modi: seriale o parallela, sincrona o asincrona, con controllo di flusso hardware o secondo diversi protocolli software.

12.2.1 Trasmissione seriale o parallela

Il modo più semplice per trasmettere un gruppo di 8 bit consiste nell'utilizzare 8 canali trasmissivi, su cui inviare gli 8 bit contemporaneamente. Gli 8 canali trasmissivi possono essere rappresentati da 8 coppie di fili o da 8 fili singoli più un filo comune come riferimento di tensione. Questo tipo di trasmissione prende il nome di trasmissione parallela. La trasmissione seriale, invece, richiede un solo

canale trasmissivo, ad esempio una coppia di fili, su cui vengono inviati consecutivamente gli 8 bit.

La figura 12.1 schematizza questi due tipi di trasmissione. Si osservi che nella trasmissione parallela i caratteri (byte) sono inviati serialmente, e i bit in parallelo; nella trasmissione seriale, sia i caratteri che i bit di ogni carattere sono trasmessi sequenzialmente.

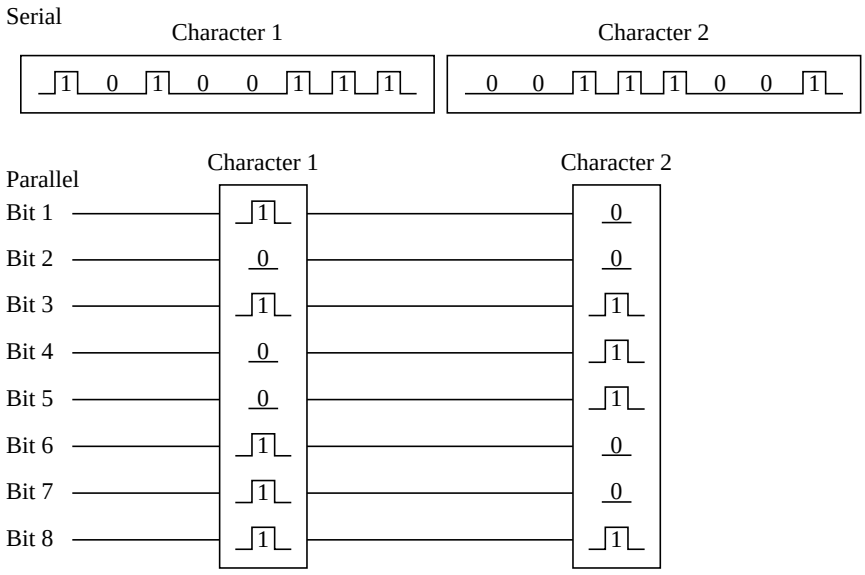


Fig. 12.1 - Trasmissione seriale e parallela.

La trasmissione parallela semplifica la circuiteria dell'interfaccia in quanto non richiede la conversione dei byte in una sequenza di bit, e consente velocità di trasmissione più elevate della seriale, ma la quantità di conduttori necessaria ne fa crescere rapidamente il costo al crescere della distanza. Pertanto, il suo utilizzo è limitato al collegamento di computer e unità periferiche su breve distanza, come nel caso dell'interfaccia Centronics per le stampanti.

12.2.2 Trasmissione sincrona o asincrona

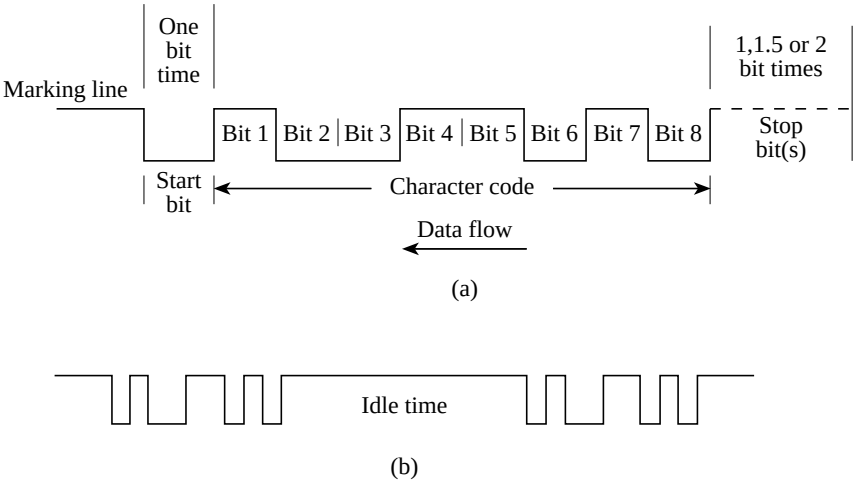
La trasmissione seriale può essere sincrona o asincrona. La trasmissione asincrona prevede che venga trasmesso e ricevuto un byte alla volta. Bit aggiuntivi rispetto all'informazione da trasmettere, detti di start e di stop, permettono di

sincronizzare il ricevitore con il trasmettitore e di separare la trasmissione dei singoli byte. La trasmissione sincrona prevede l'impacchettamento dei byte da trasmettere in trame contenenti byte aggiuntivi di sincronismo.

Trasmissione asincrona

Storicamente la trasmissione asincrona deriva dalla necessità di collegamento delle telescriventi. I caratteri provengono dalla tastiera a intervalli casuali, dipendenti dalla pressione delle dita dell'operatore sui tasti. È quindi necessario un sistema di trasmissione che permetta al ricevitore di decodificare correttamente i dati anche quando l'intervallo che intercorre tra la loro trasmissione non è un multiplo intero del tempo di bit (cioè della durata della trasmissione di un bit).

Per fare ciò, al termine della trasmissione di un byte viene inviato un bit di stop, la cui durata *minima* può essere 1, 1.5 o 2 tempi di bit. Il bit di stop è normalmente rappresentato dallo stato 1 logico sulla linea (*mark*). Lo stesso stato indica la linea *idle*, cioè in assenza di trasmissione. In pratica il bit di stop viene prolungato finché non inizia la trasmissione del byte successivo. Per permettere al ricevitore di sincronizzarsi, prima del primo bit di dato viene trasmesso un bit di start, rappresentato da una transizione dallo stato logico 1 allo stato logico 0 della linea (*space*) per la durata di un tempo di bit. Poi vengono inviati i bit di dato e l'eventuale bit di parità (figura 12.2).



(a): trasmissione di un singolo carattere;
(b): trasmissione di una sequenza di caratteri.

Fig. 12.2 - Trasmissione asincrona.

Trasmissione sincrona

Nella trasmissione sincrona i dati sono inviati tramite un continuo flusso di bit (trama). Per mantenere il ricevitore sincronizzato con il trasmettitore, ogni blocco di dati è preceduto da uno o più caratteri di sincronismo, in genere codificati con una sequenza di uni e zeri che li identificano univocamente come tali. Il ricevitore ricava dai caratteri di sincronismo un segnale di clock locale che pilota la lettura dei bit durante la ricezione del blocco di dati.

La trasmissione sincrona richiede circuiti più complessi e costosi sia per la bufferizzazione dei dati sia per la generazione del segnale di clock che deve essere sufficientemente stabile da rimanere in fase con il trasmettitore almeno per tutto il tempo che intercorre tra la trasmissione di un gruppo di byte di sincronismo e il successivo.

12.2.3 Controllo di flusso

Il controllo di flusso (handshake) consente al dispositivo ricevitore di segnalare al trasmettitore la richiesta di interrompere o riprendere la trasmissione. Questo è necessario perché è possibile che il ricevitore processi i dati in arrivo più lentamente di quanto il trasmettitore li generi. Casi tipici sono rappresentati dal collegamento computer-stampante, computer-monitor del terminale, computer-computer quando lavorano a velocità diverse.

Esistono principalmente tre meccanismi di controllo di flusso: segnali hardware RTS/CTS (spesso detto *handshake hardware*), e trasmissione dei caratteri XON/XOFF o ENQ/ACK.

RTS/CTS

Molte interfacce seriali dispongono di una coppia di fili corrispondenti ai segnali RTS (*Request To Send*) e CTS (*Clear To Send*). Quando un dispositivo ricevente rileva l'attivazione del segnale RTS da parte del dispositivo trasmittente ed è pronto per ricevere, allora risponde attivando il CTS. Per interrompere l'invio dei dati da parte del trasmettitore, il ricevitore può disattivare il segnale CTS, e riattivarlo quando sarà nuovamente in grado di ricevere i dati.

XON/XOFF

L'utilizzo dei caratteri XON e XOFF (codici 17 e 19 della tabella ASCII, talvolta identificati come DC1 e DC3 - *device control* numero 1 e 3 - e corrispondenti ai codici di controllo CTRL-Q e CTRL-S) permette di realizzare un controllo di flusso senza bisogno di segnali hardware dedicati, in quanto XON e XOFF viaggiano sugli stessi

canali dei dati. Il ricevitore trasmette un XOFF quando non è più in grado di ricevere i dati e un XON quando è nuovamente in grado di riceverli (figura 12.3).

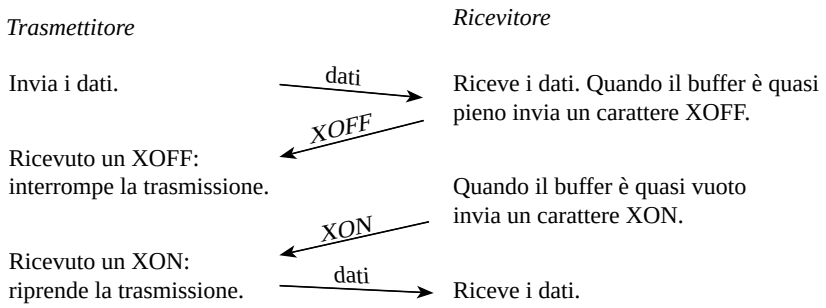


Fig. 12.3 - Protocollo XON/XOFF.

Un problema associato all'uso del controllo di flusso XON/XOFF è dovuto al fatto che i codici corrispondenti a tali caratteri possono essere presenti all'interno di file di dati di comuni programmi applicativi e, durante il trasferimento, possono provocare la sospensione all'infinito della trasmissione. Per esempio, il ben noto word processor WordStar usa il carattere CTRL-S per identificare l'inizio e la fine delle sottolineature.

ENQ/ACK

Il controllo di flusso mediante i caratteri ENQ (Enquire) e ACK (Acknowledge) è utilizzato principalmente in ambiente Hewlett Packard. A differenza di XON e XOFF, si tratta di un controllo di flusso orientato alla trasmissione dei dati a blocchi. Il trasmettitore invia un ENQ quando ha pronto un blocco di dati da trasmettere, ed attende l'ACK prima di effettuare la trasmissione (figura 12.4). Avendo predefinito la massima dimensione del blocco di dati (in genere circa 2000 byte), si previene la saturazione del buffer del ricevitore.

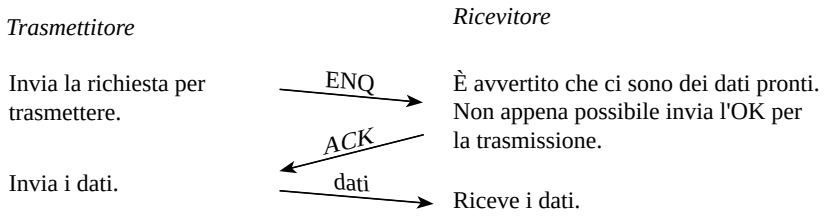


Fig. 12.4 - Protocollo ENQ/ACK.

12.2.4 RS-232

Lo standard più diffuso per il collegamento DTE-DCE è senza dubbio l'EIA RS-232-C. RS sta per "reccommended standard", e la C rappresenta la revisione. Tale standard è stato pubblicato nel 1969, e verso la fine degli anni '70 sarebbe dovuto essere rimpiazzato dagli standard RS-449, RS-422 e RS-423, progettati per maggiori velocità e più numerose funzionalità. Tuttavia, il mercato non accettò tali standard come previsto, e nel gennaio 1987 fu pubblicata la nuova revisione dello standard RS-232, l'RS-232-D, insieme ad un nuovo standard, l'RS-530. Al di fuori degli Stati Uniti lo standard RS-232 è stato recepito dal CCITT che ne ha pubblicato uno molto simile, il V.24, affiancato dal V.28 per le caratteristiche dei segnali elettrici.

Connettore

L'RS-232-D e il V.24 specificano formalmente le caratteristiche dell'ormai diffusissimo connettore a 25 pin di figura 12.5. Tale connettore, detto "a D", era già uno standard *de facto* al momento della pubblicazione degli standard. Infatti era già citato nello standard RS-232-C, anche se soltanto in una appendice. Non essendo formalmente parte dello standard, tuttavia, sono state realizzate interfacce RS-232-C con connettori diversi. Il più comune è probabilmente il connettore a D a 9 poli presente in quasi tutti i personal computer.

Normalmente il connettore "femmina" è presente sul modem (il DCE), e il connettore "maschio" sul DTE.

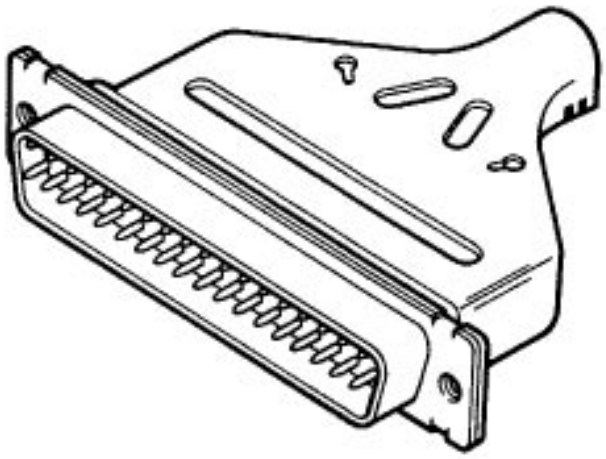


Fig. 12.5 - Connettore a D a 25 pin per RS-232-D.

Modello di riferimento

Il tipo di collegamento a cui si riferiscono gli standard RS-232 e V.24 è quello di un DTE, ad esempio un terminale, collegato mediante un cavo ad un DCE, tipicamente un modem esterno. Gli standard si applicano al trasferimento dati seriale fino a 19200 b/s, ad una distanza massima di 50 piedi (circa 16.5 metri). Questo limite è però funzione delle caratteristiche elettriche del cavo e della velocità di trasmissione, e può essere spesso superato senza problemi.

Segnali

L'RS-232 specifica 25 circuiti, ma molto spesso soltanto una piccola parte di essi servono per le comuni applicazioni pratiche.

La corrispondenza tra valori di tensione e valori logici dei segnali è riportata in tabella 12.1. Tensioni comprese tra -3V e +3V rappresentano una regione di transizione e non sono riconosciute come segnali validi.

	$-15V < v < -3V$	$3V < v < 15V$
Valore logico	1	0
Stato del segnale	Mark	Space
Funzione	OFF	ON

Tab. 12.1 - Codifica elettrica degli stati binari.

Va osservato che, a differenza degli standard RS-232, lo standard V.24 specifica principalmente come agiscono i circuiti di interfaccia, mentre è lo standard V.28 a specificare le caratteristiche elettriche dei segnali.

L'elenco completo dei segnali RS-232 è riportato in tabella 12.2, in cui in parentesi sono riportate le modifiche introdotte dalla revisione D rispetto all'RS-232-C. Esistono diversi modi per identificare ogni circuito: piedino del connettore a cui è collegato, descrizione, codice *interchange circuit* (una codifica poco mnemonica e raramente utilizzata), codice CCITT. Molto spesso si usano anche delle abbreviazioni (non standard) della descrizione: TD per *Transmitted Data*, RD per *Received Data*, SG per *Signal Ground* ecc.

PIN number	CCITT circuit	Description	Gnd	Data		Control		Timing		Testing	
				From DCE	To DCE	From DCE	To DCE	From DCE	To DCE	From DCE	To DCE
1	101	Protective Ground	x								
7	102	Signal Ground/Common Return	x								
2	103	Transmitted Data			x						
3	104	Received Data		x							
4	105	Request To Send					x				
5	106	Clear To Send				x					
6	107	Data Set Ready (DCE Ready)				x					
20	108.2	Data Terminal Ready (DTE Ready)					x				
22	125	Ring Indicator				x					
8	109	Received Line Signal Detector				x					
21	110	(Remote Loopback)/Signal Quality Detector				x					
23	111	Data Signal Rate Selector (DTE)					x				
23	112	Data Signal Rate Selector (DCE)				x					
24	113	Transmitter Signal Element Timing (DTE)							x		
15	114	Transmitter Signal Element Timing (DCE)						x			
17	115	Receiver Signal Element Timing (DCE)						x			
14	118	Secondary Transmitted Data			x						
16	119	Secondary Received Data		x							
19	120	Secondary Request To Send					x				
13	121	Secondary Clear To Send				x					
12	122	Secondary Received Line Signal Detector				x					
8	-	Reserved for testing									x
9	-	Reserved for testing								x	
18	-	(Local Loopback)									x
25	-	(Test Mode)								x	

Tab. 12.2 - Circuiti di interfaccia RS232.

In figura 12.6 sono riportati i segnali con la piedinatura nel connettore a D definita dallo standard.

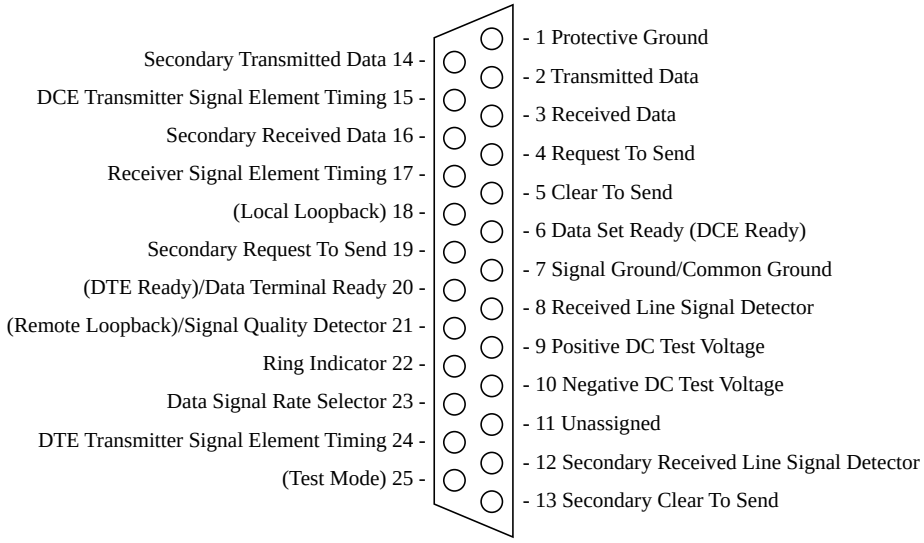

Secondary Transmitted Data 14 -
DCE Transmitter Signal Element Timing 15 -
Secondary Received Data 16 -
Receiver Signal Element Timing 17 -
(Local Loopback) 18 -
Secondary Request To Send 19 -
(DTE Ready)/Data Terminal Ready 20 -
(Remote Loopback)/Signal Quality Detector 21 -
Ring Indicator 22 -
Data Signal Rate Selector 23 -
DTE Transmitter Signal Element Timing 24 -
(Test Mode) 25 -
- 1 Protective Ground
- 2 Transmitted Data
- 3 Received Data
- 4 Request To Send
- 5 Clear To Send
- 6 Data Set Ready (DCE Ready)
- 7 Signal Ground/Common Ground
- 8 Received Line Signal Detector
- 9 Positive DC Test Voltage
- 10 Negative DC Test Voltage
- 11 Unassigned
- 12 Secondary Received Line Signal Detector
- 13 Secondary Clear To Send

Fig. 12.6 - Piedinatura RS-232-D.

I segnali principali della RS-232 sono di seguito descritti.

Massa di protezione (GND, pin 1)

Normalmente collegato alla massa (contenitore metallico) dell'apparecchiatura. Lo standard RS-232-D ne prevede l'utilizzo per il collegamento dello schermo del cavo ai fini della riduzione delle interferenze elettromagnetiche.

Signal Ground (SG, pin 7)

Questo circuito deve essere sempre collegato in qualsiasi cavo RS-232 in quanto rappresenta il riferimento di tensione di tutti i segnali. Essendoci quindi un unico riferimento, e non uno per ogni segnale, la trasmissione è di tipo sbilanciato.

Transmitted Data (TD, pin 2)

È il circuito su cui il DTE trasmette i dati al DCE. In assenza di dati si trova nello stato 1 logico (*mark*).

Received Data (RD, pin 3)

È il circuito su cui il DCE trasmette i dati al DTE. In assenza di dati si trova nello stato 1 logico (*mark*).

Request To Send (RTS, pin 4)

Con questo segnale il DTE avverte il DCE che ci sono dati da trasmettere. Il DTE attenderà il segnale CTS prima di iniziare la trasmissione.

Clear To Send (CTS, pin 5)

Con questo segnale (quando posto a ON) il DCE abilita il DTE a trasmettere i dati. Se necessario, può riportarlo a OFF per interrompere la trasmissione. Normalmente i modem attivano il CTS dopo aver ricevuto un RTS dal DTE.

Received Line Signal Detector (Carrier Detect, CD, pin 8)

Con questo segnale il modem notifica al DTE che sta ricevendo la portante dal modem remoto. Il software di comunicazione può campionare il CD per notificare all'utente un'eventuale caduta del collegamento.

Data Set Ready (DSR, pin 6)

Quando questo segnale, inviato dal DCE al DTE, è nello stato ON, il modem è collegato alla linea telefonica e pronto a trasmettere i dati. Nello standard RS-232-D questo segnale è stato ribattezzato *DCE ready*.

Data Terminal Ready (DTR, pin 20)

Segnale analogo al DSR, ma dal DTE al DCE. Diventando attivo (ON) avverte il modem di prepararsi al collegamento. Se va ad OFF il modem fa cadere automaticamente la comunicazione. Nello standard RS-232-D questo segnale è stato ribattezzato *DTE ready*.

Ring Indicator (RI, pin 22)

Segnale inviato dal DCE al DTE per notificare la ricezione di un segnale di chiamata. È utilizzato dai modem *auto-answer* (a risposta automatica) per attivare i DTE ad essi collegati.

Signal Quality Detector (CG, pin 21) e Data Signal Rate Detector (CH/CI pin 23)

Il segnale CG permette al modem di segnalare al DTE che la qualità della trasmissione è scesa sotto una certa soglia determinando così un'elevata probabilità di errore nei dati ricevuti. Tale segnale resta a ON finché la qualità è accettabile. Con il segnale sul pin 23 il DTE o il DCE (a seconda della configurazione) possono richiedere un abbassamento della velocità di trasmissione per ridurre la probabilità di errore (naturalmente soltanto quando questa funzionalità è disponibile nel modem).

Lo standard RS-232 prevede anche la modalità di trasmissione sincrona. I pin 15, 17 e 24 permettono di trasferire tra DCE e DTE segnali di clock. Normalmente, un modem in modalità sincrona pone un segnale di clock di frequenza pari a quella

di trasmissione dei bit sul pin 15, spesso detto clock di trasmissione. Il DTE usa quindi tale clock per sincronizzare la trasmissione dei dati sul pin 2. Quando il modem riceve i dati dalla linea telefonica, pone sul pin 17 il segnale di clock ricostruito al suo interno dai circuiti di sincronizzazione. Tale segnale è comunemente detto clock di ricezione. Talvolta è il DTE a fornire il clock di trasmissione al DCE, e in tal caso utilizza il pin 24. A seconda dei casi, quindi, il DTE o il DCE dovranno essere configurati in modalità "internal timing" l'uno e "external timing" l'altro.

Come si può osservare dalla tabella 12.2, sono previsti anche circuiti secondari. Si tratta della possibilità di trasmettere e ricevere su un canale secondario contemporaneamente al canale principale, normalmente ad una velocità pari ad una frazione di quella del canale principale. Le funzionalità di questi circuiti (pin 12, 13, 14, 16 e 19) sono del tutto analoghe a quelle dei circuiti primari.

Infine, lo standard RS-232-D ha aggiunto tre segnali di test: *Remote Loopback* (RL, pin 21, in alternativa all'uso come Signal Quality Detector), *Local Loopback* (LL, pin 18) e *Test Mode* (TM, pin 25).

Convertitori e adattatori

Lo standard RS-232 è pensato per interconnettere con un cavo "modem" un DTE e un DCE. Il cavo modem è un cavo "pin-to-pin" (pin 1 con pin 1, pin 2 con pin 2, ecc.). Altri tipi di cavi sono importanti per realizzare i collegamenti in alcuni casi particolari, ma non per questo poco frequenti: il collegamento tra interfacce con connettori diversi dal D a 25 pin e il collegamento null-modem.

Il collegamento più frequente tra connettori diversi è rappresentato dal 25 pin - 9 pin, quest'ultimo, come detto, presente su numerosi personal computer. La tabella 12.3 riporta la corrispondenza dei segnali.

9 pin		25 pin
1	Carrier Detect	8
2	Received Data	3
3	Transmitted Data	2
4	Data Terminal Ready	20
5	Signal Ground	7
6	Data Set Ready	6
7	Request To Send	4
8	Clear To Send	5
9	Ring Indicator	22

Tab. 12.3 - Corrispondenza dei circuiti di interfaccia.

Un altro caso molto frequente è quello del collegamento diretto tra due computer tramite cavo RS-232. Esistono diversi programmi che consentono di trasferire file in questo modo, o condividere dischi e stampanti. Il problema è che entrambi i connettori sono maschi e in entrambi, per esempio, la trasmissione dei dati avviene sul piedino 2. È ovvio che un cavo pin-to-pin non può funzionare.

Un collegamento di questo tipo prende il nome di "null-modem", in quanto viola il modello di riferimento DTE-DCE dello standard. Per realizzarlo è necessario "incrociare" tutti i segnali ad eccezione del GND e del SG (figura 12.7).

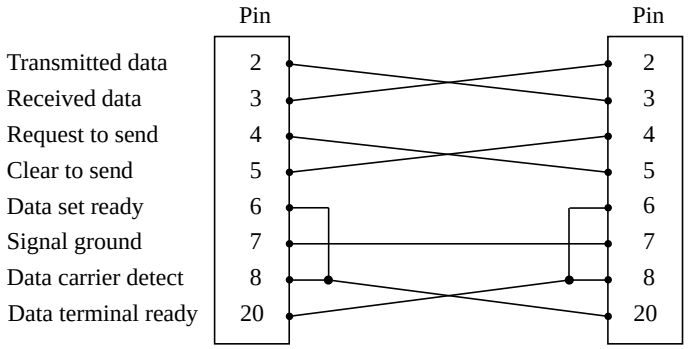


Fig. 12.7 - Esempio di cavo RS-232-D null-modem.

Non essendoci un modem, il segnale CD va generato a partire da qualche altro sicuramente attivo, per esempio dal DTR dell'altra interfaccia. In realtà, spesso è possibile configurare le interfacce RS-232 e i programmi di comunicazione per funzionare in modalità "modem" o no; in questo modo viene automaticamente disabilitata la lettura del segnale CD e questo collegamento non è necessario. Inoltre, poiché spesso la velocità di utilizzo dei dati da parte del ricevitore è superiore a quella di trasferimento, oppure il software gestisce il controllo di flusso tramite XON/XOFF, anche il collegamento incrociato di RTS e CTS è superfluo, e RTS e CTS possono essere ponticellati (figura 12.8).

È anche possibile realizzare un cavo null-modem tra un connettore a 25 pin e uno a 9, o tra due connettori a 9 pin (figure 12.9 e 12.10).

Talvolta i segnali di controllo e di handshake hardware sono superflui, e un cavo a tre conduttori può essere sufficiente. In tal caso, tutti i segnali di controllo sono ponticellati in locale (figura 12.11).

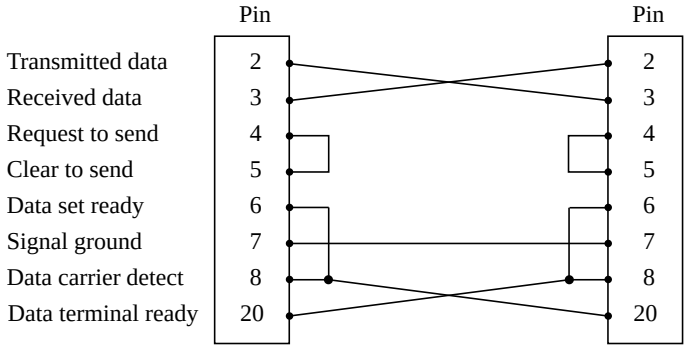


Fig. 12.8 - Esempio di cavo RS-232-D null-modem senza handshake hardware.

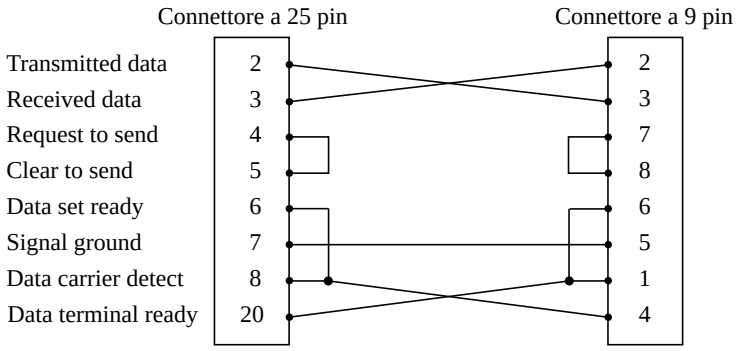


Fig. 12.9 - Esempio di cavo RS-232 null-modem tra un connettore a 25 pin e uno a 9 pin.

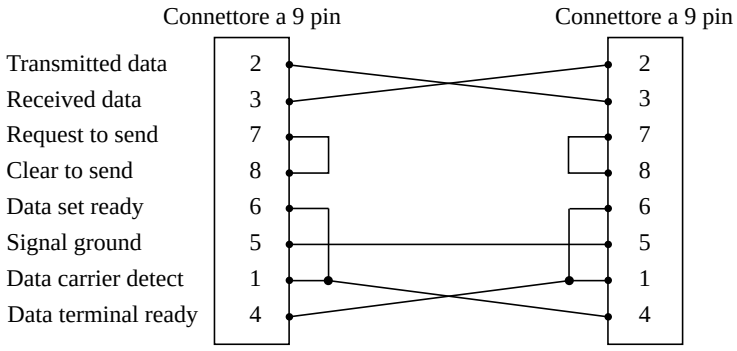


Fig. 12.10 - Esempio di cavo RS-232 null-modem a 9 pin.

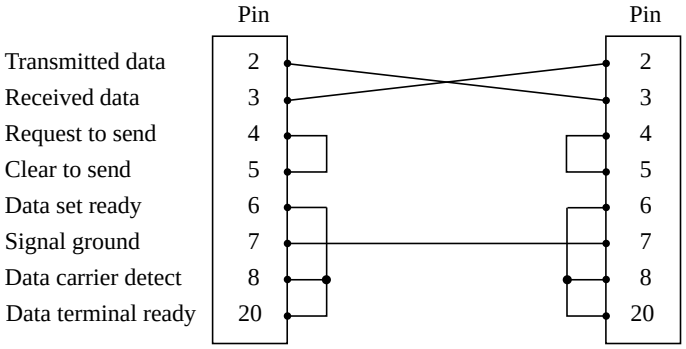


Fig. 12.11 - Cavo RS-232-D null-modem a tre fili.

Il risparmio ottenibile eliminando anche dall'hardware i circuiti di interfaccia non indispensabili può essere considerevole per le applicazioni in cui devono essere installate numerose interfacce, come nel caso dei terminal server. È così frequente trovare interfacce seriali realizzate su connettori MMJ (figura 12.12) secondo lo standard RS-423 (si veda il paragrafo 12.2.5).

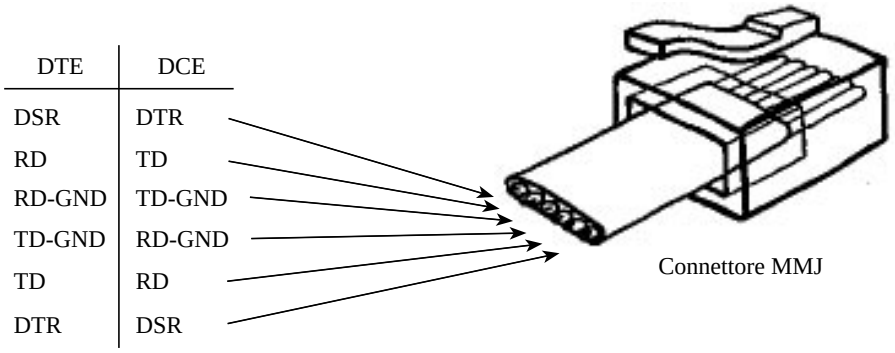


Fig. 12.12 - Interfaccia seriale su connettore MMJ.

Il connettore MMJ è di piccole dimensioni, in plastica e si monta tramite crimpatura. Questo, insieme al ridotto numero di circuiti di interfaccia presenti, ne determina il basso costo. Inoltre, data la particolare disposizione dei segnali e l'utilizzo di un cavo a piattina da 6 poli, la realizzazione di un cavo null-modem è estremamente semplice: è sufficiente torcere di 180° il cavo prima di crimpare il secondo connettore. Naturalmente, non essendo disponibili i segnali RTS e CTS, è necessario l'utilizzo di handshake tramite XON/XOFF.

Limiti dello standard RS-232/V.24

Le specifiche elettriche dei segnali definite dagli standard RS-232 e V.28 (utilizzabile per il V.24), determinano limitazioni piuttosto stringenti sulla massima velocità di trasmissione e sulla massima lunghezza dei collegamenti. Gli standard si limitano ad una velocità di 19.2 Kb/s ad una distanza di 50 piedi. In realtà, distanze maggiori possono essere coperte a minori velocità, e su cavi di pochi metri si possono raggiungere velocità superiori a 100 Kb/s.

12.2.5 RS-422, RS-423, RS-449

La ragione per cui lo standard RS-232 definisce velocità trasmissive così limitate è dovuta all'utilizzo di una tecnica trasmissiva dei segnali sbilanciata, cioè con un unico riferimento comune a 0V.

È possibile coprire maggiori distanze a velocità superiori facendo uso della trasmissione bilanciata. Con essa, ogni circuito di interfaccia è composto da due fili, e su essi il segnale è pilotato in controfase (figura 12.13).

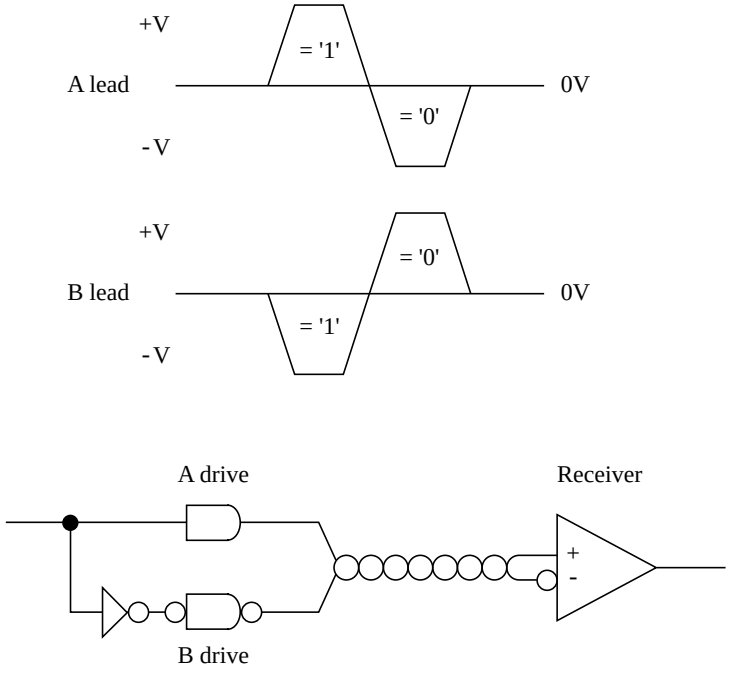


Fig. 12.13 - Tecnica di trasmissione bilanciata.

Quello illustrato è lo standard di interfaccia RS-422. A differenza della RS-232, che definisce una differenza minima di 6V tra lo 0 e l'1 logico (-3V e +3V), la RS-422 prevede soltanto 0.4V (-0.2V di differenza tra i due conduttori per l'1, +0.2V per lo 0). In questo modo è stato possibile anche ridurre l'impedenza di carico, passando dai 5 KΩ della RS-232 a 100 Ω. Infine, se la geometria dei conduttori è simmetrica, come nel caso dei doppini, il rumore elettromagnetico incidente sul cavo viene annullato in ricezione dalla lettura differenziale della tensione sui due fili. La combinazione di tutti questi fattori ha permesso di raggiungere distanze più elevate e velocità maggiori rispetto all'RS-232 (figura 12.14).

Lo standard RS-449, a differenza dell'RS-232/V.24, non specifica le caratteristiche elettriche dei segnali, ma rimanda ad altri standard quali il succitato RS-422, l'RS-442-A e l'RS-423.

L'RS-422 specifica l'utilizzo di cavi twisted pair a velocità comprese tra 100 Kb/s fino a 4000 piedi e 10 Mb/s fino a 40 piedi. L'RS-442-A e l'analogo CCITT X.27 specificano la trasmissione bilanciata tra 20 Kb/s e 10 Mb/s. L'RS-423-A e l'analogo CCITT X.26 definiscono le caratteristiche per la trasmissione sbilanciata simile all'RS-232 tra 0 e 20 Kb/s.

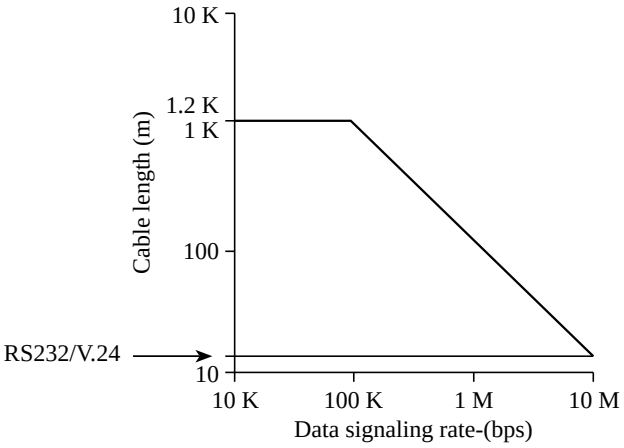


Fig. 12.14 - Distanza dei collegamenti secondo lo standard RS-422 in funzione della distanza. Per confronto è riportato anche il limite degli standard RS-232/V.24.

Lo standard RS-449 prevede l'utilizzo di un connettore a 37 pin più uno opzionale a 9 per il canale secondario. La tabella 12.4 riporta i circuiti di interfaccia; vi si riconoscono molti dei circuiti dell'RS-232-C.

RS-232-C Designation	Circuit mnemonic	Circuit name	Common		Data		Control		Timing	
			From DCE	To DCE	From DCE	To DCE	From DCE	To DCE	From DCE	To DCE
Signal Ground	SG	Signal Ground								
-	SC	Send Common		x						
-	RC	Receive Common	x							
-	IS	Terminal in Service						x		
Ring Indicator	IC	Incoming Call					x			
Data Terminal Ready	TR	Terminal Ready						x		
Data Set Ready	DM	Data Mode					x			
Transmitted Data	SD	Send Data				x				
Received Data	RD	Receive Data			x					
Transmit Timing (DTE)	TT	Terminal Timing								x
Transmit Timing (DCE)	ST	Send Timing							x	
Receive Timing	RT	Receive Timing							x	
Request To Send	RS	Request To Send						x		
Clear To Send	CS	Clear To Send					x			
Receive Signal Detector	RR	Receiver Ready					x			
Signal Quality Detector	SQ	Signal Quality					x			
-	NS	New Signal						x		
-	SF	Select Frequency						x		
Data Rate Selector (DTE)	SR	Signaling Rate Selector						x		
Data Rate Selector (DCE)	SI	Signaling Rate Indicator					x			
Secondary Transmitted Data	SSD	Secondary Send Data				x				
Secondary Received Data	SRD	Secondary Receive Data			x					
Secondary Request To Send	SRS	Secondary Request To Send						x		
Secondary Clear To Send	SCS	Secondary Clear To Send					x			
Sec. Receiver Signal Detector	SRR	Secondary Receiver Ready					x			
-	LL	Local Loopback						x		
-	RL	Remote Loopback						x		
-	TM	Test Mode					x			
-	SS	Select Standby						x		
-	SB	Standby Indicator					x			

Tab. 12.4 - Circuiti RS-449.

A causa dell'elevata complessità e dell'alto costo, l'RS-449 non ha avuto molto successo. Nel 1987 l'EIA ha pubblicato lo standard RS-530, destinato a rimpiazzare l'RS-449.

12.2.6 RS-530

Lo standard RS-530 prevede l'utilizzo del solito connettore a D a 25 pin, ma fa riferimento agli standard RS-422 e RS-423 per le caratteristiche elettriche dei segnali. Infatti, per superare il limite dei 19.2 Kb/s dell'RS-232, arrivando fino a 2 Mb/s, utilizza la trasmissione bilanciata, sacrificando diversi segnali secondari e il Ring Indicator della RS-232.

12.2.7 V.35

Lo standard più diffuso per interfacce ad alta velocità, da 48 Kb/s a 2 Mb/s, è il V.35. Utilizza una combinazione di trasmissione sbilanciata per i segnali di controllo e bilanciata per i dati e i segnali di clock. Il connettore previsto è l'ISO 2593 (figura 12.15), a 34 pin.

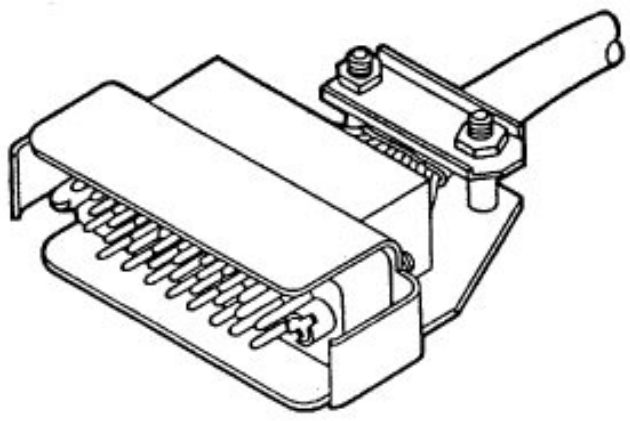


Fig. 12.15 - Connettore per l'interfaccia V.35.

La tabella 12.5 riporta i segnali di interfaccia V.35.

PIN	Circuit name	Description	From DCE	To DCE
A	FG	Frame Ground		
B	SG	Signal Ground		
C	RTS	Request To Send	x	
D	CTS	Clear To Send		x
E	DSR	Data Set Ready	x	
F	RLSD	Received Line Signal Detector	x	
H	DTR	Data Terminal Ready		x
J	RI	Ring Indicator	x	
R/T	RD	Receive Data	x	
U/X	SGR	Receive Clock	x	
P/S	SD	Send Data		x
U/W	SCTE	Send Clock (EXT)		x
Y/A	SCT	Send Clock	x	
m	TST	Reserved for Test	x	

Tab. 12.5 - Circuiti di interfaccia V.35.

12.3 MODEM

I modem consentono di adattare il segnale digitale proveniente da un'interfaccia seriale ad un canale trasmissivo limitato in banda sia inferiormente che superiormente. Il caso più comune è quello del canale telefonico. Un canale telefonico presenta una banda passante di circa 3000 Hz, tra 300 e 3300 Hz (figura 12.16).

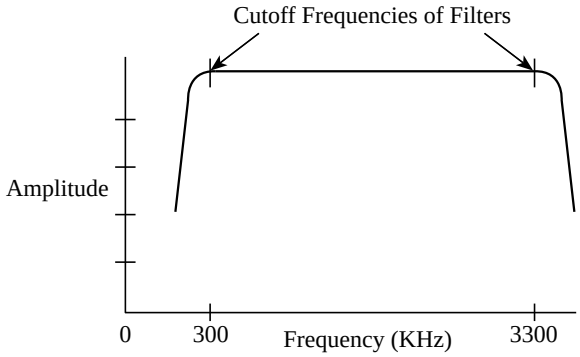


Fig. 12.16 - Risposta in frequenza di un tipico canale telefonico.

Benché circa sette volte inferiore all'intervallo di frequenze udibili dall'orecchio umano, questa banda passante è sufficiente per rendere comprensibile la voce umana, e consente un maggior sfruttamento dei canali a larga banda tramite tecniche FDM o TDM. Questa larghezza di banda limita la massima velocità trasmissiva. Inoltre, essendoci una frequenza di taglio inferiore a 300 Hz, non è possibile trasmettere la corrente continua. Un sequenza di cifre binarie uguali, o lo stato di idle della linea, sono codificate dagli standard per interfacce seriali proprio come tensioni fisse ad un certo valore, cioè corrente continua. È pertanto necessario modificare la codifica dei bit. I modem fanno questo tramite tecniche di modulazione, da cui il nome (modem = MOdulatore-DEModulatore).

12.3.1 Tecniche di modulazione

Oltre al segnale vocale, un qualsiasi segnale di frequenza compresa all'interno della banda passante del canale telefonico è adatto per essere trasmesso su di esso. Il segnale più adatto per la modulazione è un segnale sinusoidale, rappresentabile dall'espressione:

$$s(t) = \mathrm{A} \sin (2\pi ft + \varphi)$$

in cui si individuano tre parametri del segnale: l'ampiezza *A*, la frequenza *f* e la fase φ. Facendo variare nel tempo uno più di questi parametri si può usare il segnale sinusoidale per trasmettere informazione. Modificando l'ampiezza si ottiene la *modulazione di ampiezza* (AM), modificando la frequenza si ha la *modulazione di frequenza* (FM), e modificando la fase la *modulazione di fase* (PM).

Modulazione di ampiezza

La modulazione di ampiezza è la più semplice tecnica di modulazione (figura 12.17).

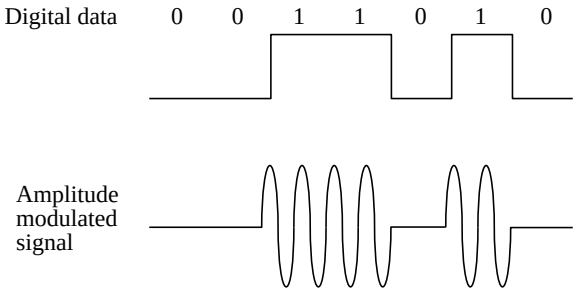


Fig. 12.17 - Modulazione di ampiezza.

Benché da sola consenta velocità trasmissive abbastanza basse, è spesso usata in unione ad altre tecniche di modulazione per sistemi ad alta velocità.

Modulazione di frequenza

Nella modulazione di frequenza, la frequenza della portante varia in funzione del segnale modulante. Nella trasmissione digitale si avranno quindi due frequenze diverse, una leggermente superiore ed una leggermente inferiore a quella della portante, per codificare gli zeri e gli uni (figura 12.18). Tale tecnica è detta *Frequency Shift Keying* (FSK).

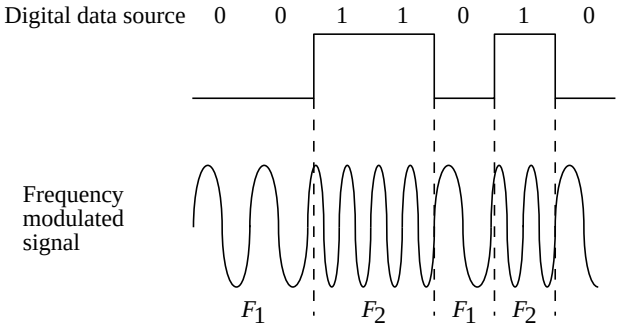


Fig. 12.18 - Modulazione di frequenza.

Modulazione di fase

Nella modulazione di fase, la portante varia la sua fase in funzione del segnale da trasmettere. Nella trasmissione digitale agli zeri e agli uno sono associati diversi valori di rotazione della fase (per esempio 90° per l'1 e 270° per lo 0), e questo prende il nome di *Phase Shift Keying* (PSK). Spesso la codifica dei bit non è riferita a valori di fase assoluti, bensì a rotazioni di fase rispetto alla fase dell'ultimo simbolo ricevuto. In questo caso si parla di *Differential Phase Shift Keying* (DPSK).

La modulazione di fase è la tecnica più costosa, ma è anche la più adatta ad essere utilizzata in combinazione alla modulazione di ampiezza per ottenere elevate velocità di trasmissione.

BAUD e b/s

Il numero di bit trasmessi nell'unità di tempo è normalmente indicato come b/s o bps (*bit per second*). Quando si utilizzano tecniche di modulazione, come nel caso dei

modem, ogni elemento del segnale portante inviato dal modem (per esempio, ma non necessariamente, un ciclo del segnale portante sinusoidale) viene detto *simbolo*. Il numero di simboli inviati dal modem nell'unità di tempo prende il nome di *baud*. Le tecniche di modulazione possono associare ad ogni simbolo uno o più bit, per esempio usando quattro od otto valori diversi per la rotazione di fase nella PSK, o utilizzando una combinazione di più modulazioni, per esempio quattro valori per la fase e due per l'ampiezza. In questo modo il numero di bit per secondo risulta essere maggiore dei baud.

Teorema di Nyquist

Nel 1928 Nyquist trovò la relazione tra la banda di un canale e la massima velocità in baud. Tale relazione è:

$$B = 2H$$

dove B è la velocità in baud (simboli al secondo) e H la banda del canale. Per un canale telefonico di banda 3000 Hz, quindi, il numero di simboli trasmissibili nell'unità di tempo è 6000. Al di sopra di tale velocità i simboli interferiscono tra di loro a causa della cosiddetta interferenza intersimbolica. Se ad ogni simbolo viene associato un bit, ad esempio con una modulazione di ampiezza, la massima velocità teorica su un canale telefonico sarà pertanto 6000 b/s (si osservi l'analogia con la figura 3.2).

Per superare questo limite occorre associare più di un bit ad ogni simbolo. Questo è possibile con tecniche di modulazione più sofisticate. La più comune tra queste è la QAM (*Quadratude Amplitude Modulation*), che prevede la modulazione contemporanea dell'ampiezza e della fase. Associando quattro bit a ogni variazione del segnale, cioè ad ogni simbolo, per una velocità di 2400 baud si ottiene una velocità di trasmissione dei dati di 9600 b/s. In figura 12.19 è rappresentato lo schema di modulazione di uno dei primi modem QAM: il 209 della Bell. La combinazione di 3 ampiezze e 12 valori di fase permetteva di codificare 4 bit in ciascun simbolo.

Teorema di Shannon

Aumentando la complessità della modulazione sembrerebbe possibile aumentare a piacere la velocità di trasmissione dei dati. In realtà questo non è possibile perché al di sopra di un certo limite i simboli non sono più distinguibili l'uno dall'altro, determinando errori di ricezione. Le ragioni possono essere diverse, per esempio la rotazione di fase introdotta dal canale trasmissivo, la non linearità degli amplificatori o il rumore della linea.

Shannon, nel 1948, introdusse nel risultato di Nyquist il rumore come fattore limitante della modulazione, ottenendo per la velocità di trasmissione dei dati la

seguente espressione:

$$R = H \log_2 (1 + S/N)$$

dove H è la banda del canale e S/N è il rapporto segnale/rumore. Per un canale telefonico di 3000 Hz con un rapporto S/N di 30 dB (pari a 1000) si ottiene una velocità massima di circa 30000 b/s.

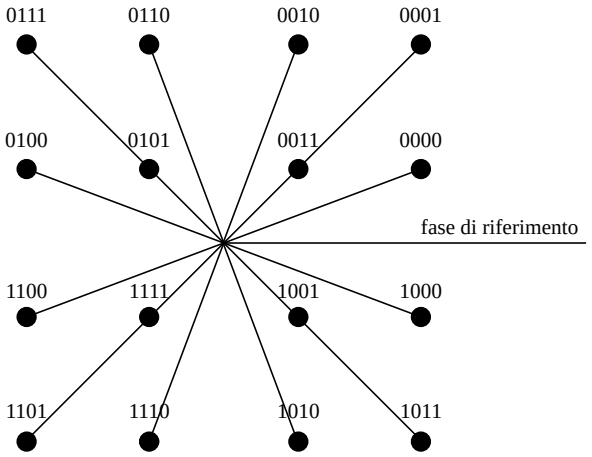


Fig. 12.19 - Costellazione dei simboli nella modulazione QAM a 3 ampiezze e 12 valori di fase.

Trellis Coded Modulation

La modulazione QAM consente trasmissioni fino a 14400 b/s, ma soltanto su linee di buona qualità. Su linee abbastanza disturbate, la quantità di ritrasmissioni necessarie può rendere più efficiente lavorare a 9600 b/s. La *Trellis Coded Modulation* (TCM) permette di tollerare un rumore doppio rispetto a quello massimo tollerabile dalla QAM.

Gli errori nella trasmissione QAM sono dovuti allo spostamento del segnale ricevuto da un punto della "costellazione" della codifica (figura 12.19) ad un altro a causa di rumore, distorsioni di ampiezza e rotazioni di fase. Per minimizzare questa eventualità la TCM introduce un bit di ridondanza nella codifica di ciascun simbolo. In una trasmissione a 14400 b/s, 6 bit di dato più uno di ridondanza sono codificati in ciascun simbolo, dando luogo ad una costellazione di 128 punti. La TCM

prevede la *Forward Error Correction* (FEC) grazie ad una codifica convoluzionale, in base alla quale ogni bit viene confrontato con uno o più bit trasmessi prima, e il suo valore dipende anche da essi.

12.3.2 Trasmissione half-duplex e full-duplex

Si definisce una trasmissione *half-duplex* quando essa avviene alternativamente in un senso e nell'altro. La ragione è dovuta alla necessità di condividere il medesimo canale trasmissivo da parte delle due stazioni collegate, come nel caso dei "walkie-talkie", in cui la commutazione tra trasmissione e ricezione avviene quasi sempre manualmente in seguito ad una parola convenzionale ("passo"). Nei modem il canale trasmissivo condiviso è quello telefonico. Benché i collegamenti all'interno delle centrali telefoniche e tra le centrali stesse siano realizzati con canali indipendenti per la trasmissione e la ricezione, il collegamento verso l'utente finale usa soltanto due fili e le voci dei due interlocutori si sovrappongono negli auricolari dei microtelefoni.

I circuiti di demodulazione dei modem hanno naturalmente difficoltà a decodificare un segnale quando ad esso ne è sovrapposto un altro. Per questo i primi collegamenti funzionavano in half-duplex: a turno, ciascun modem poteva utilizzare completamente il canale.

La trasmissione half-duplex presenta lo svantaggio di introdurre un overhead dovuto alla commutazione tra trasmissione e ricezione. Per collegamenti altamente interattivi, o quando si usano protocolli che prevedono frequenti messaggi di acknowledge, tale overhead può diventare inaccettabile ed è necessario adottare tecniche *full-duplex*. La tecnica più diffusa per la comunicazione in full-duplex consiste nella suddivisione della banda del canale in due parti: ciascun modem ne userà una per trasmettere e l'altra per ricevere. Questo avviene utilizzando frequenze portanti diverse per i due modem, e ciascuno in ricezione filtrerà il segnale in modo da sopprimere l'eco della propria trasmissione (figura 12.20, in cui è riportata l'assegnazione delle frequenze per lo standard V.21).

Questo comporta naturalmente che i due modem siano configurati in modo speculare: l'uno in modalità "call" o "originate", l'altro in modo "answer". I modem moderni a chiamata e risposta automatica sono in grado di effettuare automaticamente questa configurazione.

La divisione in due della banda consente velocità di trasmissioni fino a 2400 b/s in full-duplex, ma impedisce velocità superiori in quanto il canale effettivo utilizzabile risulta in pratica dimezzato. Lo sviluppo di circuiti integrati VLSI ed in particolare dei

DSP (Digital Signal Processor) ha consentito la realizzazione di modem full-duplex basati sulla tecnica di cancellazione dell'eco. I due modem usano entrambi tutta la banda del canale, cosa che normalmente genererebbe interferenza tra le portanti. Tuttavia, ciascuno è in grado di cancellare in ricezione gli effetti della propria trasmissione, isolando quindi il segnale proveniente dall'altro modem.

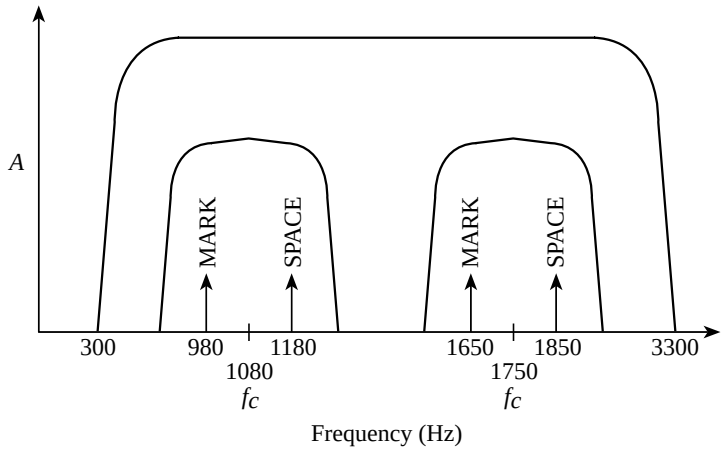


Fig. 12.20 - Utilizzazione del canale nello standard V.21.

12.3.3 Standard

Nel seguito saranno illustrati alcuni dei principali standard CCITT per i modem. La tabella 12.6 riporta le caratteristiche essenziali dei principali standard CCITT e Bell System (questi ultimi in uso negli Stati Uniti).

modem	velocità massima (bps)	Trasmissione (s = sincrona, a = asincrona)	Tecnica di modulazione	Trasmissione (h = half-duplex, f = full-duplex)	Linea (c = commutata, d = dedicata)
BELL SYSTEM					
103A,E	300	A	FSK	H, F	C
103F	300	A	FSK	H, F	D
201B	2400	S	PSK	H, F	D
201C	2400	S	PSK	H, F	C
202C	1200	A	FSK	H	C
202S	1200	A	FSK	H	C
202D/R	1800	A	FSK	H, F	D
202T	1800	A	FSK	H, F	D
208A	4800	S	PSK	H, F	D
208B	4800	S	PSK	H	C
209A	9600	S	QAM	F	D
212	300	A	FSK	H, F	C
CCITT					
V.21	300	A	FSK	H, F	C
V.22	600	A	PSK	H, F	C, D
	1200	A, S	PSK	H, F	C, D
V.22 bis	2400	A	QAM	H, F	C
V.23	600	A, S	FSK	H, F	C
	1200	A, S	FSK	H, F	C
V.26	2400	S	PSK	H, F	D
	1200	S	PSK	H	C
V.26 bis	2400	S	PSK	H	C
V.26 ter	2400	S	PSK	H, F	C
V.27	4800	S	PSK	H, F	D
V.29	9600	S	QAM	H, F	(privata)
V.32	9600	A	TCM/QAM	H, F	C, D
V.32 bis	14400	A	TCM/QAM	H, F	C, D
V.32 terbo	19200	A	TCM/QAM	H, F	C,D
V.33	14400	S	TCM	H, F	D
V.34	28800	A	TCM	H, F	C,D

Tab. 12.6 - Standard per modem.

V.21

Lo standard CCITT V.21 prevede il collegamento asincrono di due modem in half-duplex o in full-duplex su linea commutata a 300 b/s usando la tecnica di modulazione FSK. La tabella 12.7 riporta le frequenze con cui sono codificati gli zeri e gli uni nelle due modalità di funzionamento answer e originate.

	Originate	Answer
Mark	980 Hz	1650 Hz
Space	1180 Hz	1850 Hz

Tab. 12.7 - Frequenze V.21.

V.22

Lo standard CCITT V.22 prevede due velocità di collegamento: 1200 b/s e 600 b/s, entrambe tramite modulazione di fase. A 1200 b/s è previsto l'uso della modulazione DPSK a due bit per simbolo in modalità sincrona o asincrona. È adatto a linee commutate o dedicate in half-duplex o in full-duplex.

V.22 bis

Il V.22 bis è uno degli standard che prevedono una trasmissione a 2400 b/s half-duplex o full-duplex, sincrona o asincrona sia su linea commutata che su linea dedicata a due fili. In realtà, i due modem comunicano sempre in modo sincrono usando una modulazione QAM a 600 baud codificando quattro bit per simbolo. I primi due bit determinano la rotazione di fase (trattandosi di quattro valori possibili corrisponde ad un cambiamento di quadrante in un diagramma polare), gli altri due determinano uno di quattro simboli all'interno del quadrante.

V.23

Il V.23 è uno standard di trasmissione su linee commutate a 600 o 1200 b/s in FSK. La sua particolarità consiste nel fatto che è uno standard asimmetrico: il canale di ritorno (opzionale, lo standard prevede anche la modalità half-duplex) usa una banda molto stretta (segnale a 390 Hz per inviare un 1 e 450 per uno 0), permettendo così una velocità di soli 75 b/s. Questo canale di ritorno può essere usato per il controllo degli errori, ma soprattutto può essere usato per inviare brevi codici di comando da una tastiera. Questo è il caso tipico delle banche dati e dei sistemi guidati a menù, ed infatti il V.23 ha trovato vasta applicazione in Europa nei servizi Videotext (per esempio il Videotel Telecom Italia).

V.32

Lo standard V.32 prevede la trasmissione half-duplex o full-duplex su linee commutate o dedicate ad una velocità massima di 9600 b/s con una portante a 1800 Hz modulata a 2400 baud. La tecnica usata è una variante della QAM. Infatti, i due canali usati dai due modem per trasmettere nelle due direzioni condividono approssimativamente la stessa banda, e un circuito di cancellazione dell'eco permette di distinguere tra segnale trasmesso e segnale ricevuto. Inoltre, lo standard prevede due schemi di codifica: uno convenzionale ed uno ridondante (TCM).

V.32 bis

Questo standard presenta le stesse caratteristiche del V.32, ma con una costellazione della codifica dei simboli a 128 punti, consentendo una velocità massima di 14400 b/s. I modem V.32 bis sono compatibili con i modem V.32 e possono modificare dinamicamente la velocità di trasmissione durante il collegamento.

V.32 terbo

Rappresenta una ulteriore evoluzione del V32.bis proposta da AT&T. Usa una costellazione di 256 o 512 punti e consente una velocità massima di 19200 b/s.

V.34

Lo standard V.34 è il più recente e consente una velocità massima di 28800 b/s. Si tratta di uno standard molto sofisticato che prevede una costellazione fino a 768 punti con rilevazione automatica e dinamica delle caratteristiche del canale per adattare i parametri di trasmissione ad esse.

Rilevamento e correzione degli errori

Fino al 1989 non esistevano standard *de jure* per il rilevamento e la correzione degli errori di trasmissione nei modem, e si trovavano diverse implementazioni di codici ciclici ridondanti (CRC) simili tra di loro, ma incompatibili. L'unico standard *de facto* era rappresentato dal Microcom Network Protocol di classe 4 (MNP 4), rilasciato su licenza a numerosi costruttori. Nel 1979 il CCITT ha riconosciuto tale situazione adottando l'MNP come uno dei due protocolli per il rilevamento e la correzione degli errori definiti dallo standard V.42. Il metodo primario proposto dallo standard è invece il "Link Access Protocol-Modem" (LAP-M) che usa una differente struttura di trama ed un diverso polinomio per la generazione del CRC.

Compressione dei dati

Come accadde per la correzione degli errori, anche per la compressione dei dati si è dovuto attendere il 1990 per un standardizzazione *de jure*. Il CCITT, in tale anno, ha emesso lo standard V.42 bis, definendo il metodo di compressione, noto come Lempel-

Ziv, come standard internazionale. A differenza del V.42, il V.42 bis non riconobbe tecniche alternative, benché fossero già presenti modem con tale funzionalità. Lo standard *de facto* più diffuso è l'MNP di classe 5 che, grazie alla compatibilità verso il basso, è anche compatibile con la correzione degli errori dell'MNP di classe 4.

12.3.4 Comandi ai modem

Molti modem moderni dispongono di un microprocessore con RAM, ROM, EPROM e opportuno software per automatizzare le operazioni di configurazione, controllare i dispositivi di composizione automatica dei numeri, memorizzare numeri telefonici, gestire la compressione dei dati e la correzione degli errori. Tutte queste funzionalità sono in genere controllate tramite semplici linguaggi di comandi, dei quali il più diffuso, al punto da rappresentare un standard *de facto*, è il linguaggio Hayes, inizialmente adottato negli Smartmodem della Hayes Microcomputer Products. Il linguaggio Hayes prende anche il nome di linguaggio AT in quanto tutti i comandi iniziano per AT.

Il modem riceve i comandi dalla stessa porta seriale con cui è collegato il terminale o il computer. Pertanto interpreta i caratteri ricevuti come comandi finché non viene attivata la connessione con l'altro modem, dopodiché i caratteri non vengono più interpretati, ma trasmessi. Il fatto che tutti i comandi inizino per AT permette ai modem che dispongono di un buffer di memoria per la trasmissione di riconoscere automaticamente la velocità dei dati sull'interfaccia seriale e di adattarvisi, indipendentemente dalla velocità a cui avverrà il collegamento. Tali modem sono talvolta detti *autobaud*.

Il formato dei comandi Hayes è il seguente:

AT<comando>[<parametro>][<comando>[<parametro>] ...]

Alcuni esempi di comandi Hayes sono riportati in tabella 12.8.

Comando	Descrizione
A	answer call
D	dial the following telephone number
E	enable or inhibit the echo of command characters
H	hang-up
O	place modem on-line
Q	enable or inhibit sending of result code
S	set modem register values
Z	reset the modem
+++	escape sequence

Tab. 12.8 - Principali comandi Hayes.

Il comando di escape è un po' particolare. Quando il modem è collegato non interpreta i comandi, in quanto deve trasmettere i caratteri ricevuti dall'interfaccia seriale. Se l'utente o il programma di controllo deve ottenere il controllo del modem durante il collegamento è prevista una sequenza ravvicinata di tre caratteri '+' isolata dall'invio di altri caratteri dopo la quale l'interprete dei comandi ridiventa attivo.

Il linguaggio Hayes permette anche la modifica dei valori contenuti nei registri interni del modem, permettendo di configurare numerosi parametri di funzionamento. Per esempio, il contenuto del registro S0 determina dopo quanti squilli un modem a risposta automatica risponderà ad una chiamata in arrivo. Il comando ATS0=3 configura il modem a rispondere dopo tre squilli, il comando ATS0=0 disabilita la risposta automatica.

Dopo ogni comando l'interprete risponde con un messaggio testuale o con un codice numerico. Questo permette non soltanto all'utente di verificare l'esito dei comandi, ma anche di scrivere programmi che controllino e programmino in modo automatico i modem.

12.3.5 Sicurezza

La disponibilità di accessi via modem a banche dati, centri di calcolo e centri di servizi, spesso nodi di reti geografiche, solleva il problema della sicurezza e della necessità di prevenire accessi non autorizzati. Una tecnica efficace è quella del *callback*: effettuando la chiamata al modem non si ottiene direttamente la richiesta di login per l'accesso al servizio, ma la richiesta di identificazione dell'utente, eventualmente con password, e del numero telefonico da cui chiama. Se l'utente e il numero risultano essere stati preventivamente autorizzati all'uso della risorsa, il modem fa cadere la linea e richiama l'utente al numero fornito. In questo modo si impedisce l'accesso ad estranei o ad utenti non autorizzati, avendo una sufficiente garanzia sull'identità dell'utente. Questo procedimento può essere gestito via software su mainframe o workstation, mediante programmi che gestiscono un database di autorizzazioni e controllano automaticamente uno o più modem, ma esistono anche modem e terminal server costruiti appositamente per funzionare in questo modo, in grado di gestire utenti, numeri telefonici e procedure d'accesso in modo autonomo.

12.4 CDA, CDN, COMMUTAZIONE DI CIRCUITO E DI PACCHETTO

Le linee commutate, cioè le normali linee telefoniche, sono state basate per lungo tempo su una tecnica di commutazione detta *commutazione di circuito*. Le prime centrali telefoniche funzionavano manualmente, le operatrici collegavano a richiesta la linea dell'utente che effettuava la chiamata con l'utente desiderato. Con le centrali automatiche, dispositivi elettromeccanici effettuavano la stessa operazione comandati dal combinatore telefonico dell'apparecchio dell'utente (il disco dei vecchi modelli di telefono).

La commutazione di circuito crea quindi un vero collegamento fisico tra i due utenti, ed esso resta stabile e riservato a loro per tutta la durata della comunicazione. Questo comporta in media un basso utilizzo del canale trasmissivo, risultando occupato da una comunicazione anche quando i due interlocutori non parlano o quando i due modem non si scambiano dati. Un altro limite della commutazione di circuito è dovuto al fatto che l'insieme dei collegamenti tra le centrali e le apparecchiature (amplificatori, soppressori d'eco, ecc.) attraversate di volta in volta per mettere in comunicazione due utenti può non essere sempre lo stesso, determinando variazioni anche considerevoli nelle caratteristiche del canale.

Le linee dedicate o, più propriamente, i *Canali Diretti Analogici* (CDA) consentono in generale prestazioni migliori rispetto alle normali linee commutate in quanto sono realizzate mediante collegamenti fissi tra i due utenti e quindi senza attraversamento delle apparecchiature di commutazione all'interno delle centrali. Pertanto, anche i circuiti attivi attraversati sono sempre gli stessi, ed è quindi possibile compensare le inevitabili non linearità del canale misurandone le caratteristiche una volta per tutte. Così si possono compensare irregolarità nella banda passante e ritardi di fase in funzione della frequenza mediante la regolazione di appositi equalizzatori. Sulle linee commutate queste caratteristiche variano di volta in volta, e molti modem con velocità inferiore a 4800 b/s dispongono di equalizzatori fissi tarati per le caratteristiche medie delle linee. Per velocità superiori, la maggior parte dei modem dispone di equalizzatori automatici che, all'inizio del collegamento, misurano alcuni parametri del canale e regolano i circuiti di equalizzazione in conseguenza.

Un'altra possibilità fornita dai CDA consiste nella disponibilità di linee a quattro fili, normalmente limitatamente all'ambito urbano. Questo consente di comunicare in full-duplex usando due fili per la trasmissione e due per la ricezione. Spesso tali linee non solo sono esterne ai circuiti di commutazione delle centrali, ma non attraversano neanche gli amplificatori in banda fonica. Pertanto, è possibile utilizzare i cosiddetti modem a larga banda che, sfruttando la maggior banda passante, consentono velocità superiori.

L'alternativa alla commutazione di circuito, per un migliore utilizzo dei canali trasmissivi, è rappresentata dalla commutazione di pacchetto, basata su sistemi digitali sia per l'instradamento che per la trasmissione dei dati. In essa i pacchetti (digitali) contengono l'indirizzo del destinatario, e transitano attraverso la rete condividendo i canali trasmissivi con altre comunicazioni. In ogni nodo vengono instradati in base all'indirizzo, e arrivati al nodo finale vengono inoltrati all'utente.

La figura 12.21 mostra un esempio di rete a commutazione di pacchetto non connessa (datagram): sul computer A risiedono gli utenti A, B, C, D e sul computer B risiedono gli utenti X, Y, Z, W. Si osservi che i canali trasmissivi sono condivisi da tutti gli utenti della rete e che i pacchetti possono essere ricevuti dal nodo finale in ordine diverso da quello con cui sono stati trasmessi, e quindi è necessario che esso disponga di memoria e capacità elaborativa sufficiente a riordinarli prima di inoltrarli all'utente.

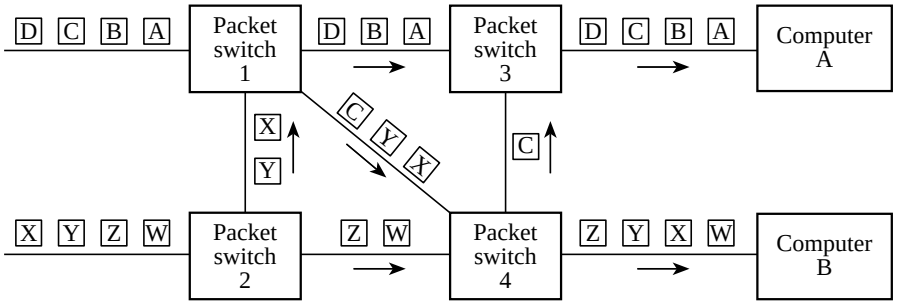


Fig. 12.21 - Flussi di dati in una rete datagram a commutazione di pacchetto.

Esistono anche reti a commutazione di pacchetto a circuiti virtuali. In esse, al momento dell'attivazione del collegamento tra due stazioni viene stabilito l'instradamento dei pacchetti attraverso tutti i nodi intermedi (cioè si crea un circuito virtuale), e tale instradamento resterà fisso per tutta la durata del collegamento. Questo permette di semplificare i nodi, in quanto i pacchetti arrivano già nell'ordine corretto, e riduce i ritardi, dovuti al loro riordinamento, tipici delle reti datagram.

Tecniche alternative per aumentare l'efficienza delle reti a commutazione di pacchetto sono le recenti "fast packet switching", "frame relay" e "cell relay" (si vedano in proposito i paragrafi 13.5 e 13.6).

Grazie al fatto che la tecnologia digitale è oggi alla base anche del traffico telefonico, i CDA vengono gradualmente rimpiazzati dai CDN: i *Canali Diretti Numerici*. Il collegamento tra le centrali avviene mediante dorsali digitali ad alta velocità condivise da più canali con tecniche TDM (*Time Division Multiplexing*).

Con i CDN è possibile sfruttare tutto o in parte il flusso di dati delle dorsali inserendo all'interno delle trame utilizzate per i canali telefonici digitali i dati degli utenti.

12.5 PDH (PLESIOCHRONOUS DIGITAL HIERARCHY)

Per trasportare un canale telefonico tramite un flusso numerico occorre codificare la voce tramite una tecnica detta PCM (*Pulse Code Modulation*). Il teorema del campionamento (anch'esso dovuto a Nyquist), dimostra che è possibile ricostruire un segnale analogico a partire da una sequenza di campioni, purché questi vengano prelevati dal segnale originale ad una frequenza maggiore o uguale al doppio della massima frequenza dello spettro di potenza del segnale stesso. Un canale vocale filtrato a 3300 Hz dai circuiti telefonici può quindi essere campionato a 8 kHz, prelevando cioè 8000 campioni al secondo (uno ogni 0.125 ms).

Per la trasmissione digitale è poi necessario associare a ciascun campione un valore numerico discreto (quantizzazione). A differenza del campionamento, questa operazione introduce un'errore di approssimazione (rumore), e quindi il numero di bit di ogni campione è funzione della qualità che si vuole ottenere: l'Europa ha scelto di operare con campioni da 8 bit, mentre gli USA hanno scelto campioni su 7 bit. La velocità di un canale telefonico digitale è quindi 64 Kb/s in Europa e 56 Kb/s negli USA.

Più canali numerici (detti tributari) possono essere raggruppati mediante tecniche TDM per formare canali più veloci (detti canali multipli). Le modalità di multiplazione sono specificate da due gerarchie: la gerarchia plesiocrona (descritta in questo paragrafo) e la gerarchia sincrona (descritta nel prossimo paragrafo).

La prima trama della gerarchia plesiocrona (*PDH: Plesiochronous Digital Hierarchy*) è negli USA la trama T1, mentre in Europa è la trama E1 (figura 12.22). Si noti come la durata delle due trame sia sempre pari a 0.125 ms, pari alla durata di un campione PCM.

La trama T1 permette l'invio di 24 canali tributari a 64 Kb/s su un canale multiplo a 1.544 Mb/s, di cui 1.536 Mb/s sono utilizzati per la trasmissione dei dati e 8 Kb/s per le informazioni di sincronismo (bit F: *Framing*). I canali tributari della trama T1 possono essere utilizzati a 56 Kb/s (soluzione idonea nel caso di canali telefonici digitali) lasciando libero l'ottavo bit che può essere dedicato a funzioni di segnalazione, oppure a 64 Kb/s (soluzione migliore nel caso di trasmissione dati) dedicando un intero canale tributario alle funzioni di segnalazione.

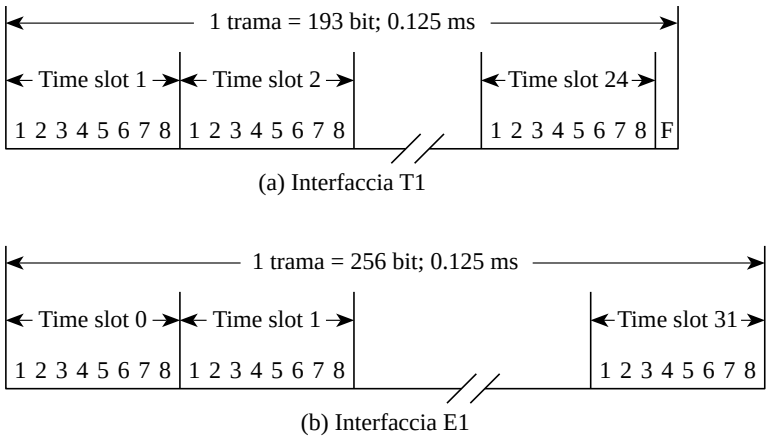

1 trama = 193 bit; 0.125 ms
Time slot 1
Time slot 2
Time slot 24
1 2 3 4 5 6 7 8
1 2 3 4 5 6 7 8
1 2 3 4 5 6 7 8
F
(a) Interfaccia T1
1 trama = 256 bit; 0.125 ms
Time slot 0
Time slot 1
Time slot 31
1 2 3 4 5 6 7 8
1 2 3 4 5 6 7 8
1 2 3 4 5 6 7 8
(b) Interfaccia E1

Fig. 12.22 - Gerarchie plesiocrone e sincrone.

La trama E1 (il cui codice tecnico è G.703/732) prevede la trasmissione di 32 canali a 64 Kb/s, di cui uno riservato al sincronismo e uno alle informazioni di controllo (tabella 12.9).

Time slot	Tipo di informazione
0	Sincronismo
1 - 15	Dati e canali telefonici PCM
16	Controllo
17 - 31	Dati e canali telefonici PCM

Tab. 12.9 - Canali trama E1.

La trasmissione dati su flussi della gerarchia plesiocrona può avvenire in due modalità: non strutturata o strutturata.

Nel collegamento non strutturato, l'apparecchiatura di interfaccia, normalmente collegata alla centrale mediante due cavi coassiali, uno per la trasmissione ed uno per la ricezione, fornisce un flusso a 2.048 Mb/s (1.544 Mb/s negli USA) senza imporre alcuna struttura di trama. L'unico vincolo è la necessità di sincronizzarsi al clock di trasmissione fornito dall'interfaccia.

Nel collegamento strutturato, invece, è necessaria la conformità alla struttura di trama E1 (T1). È anche possibile non utilizzare tutti i 30 (23) canali tributari disponibili, ottenendo canali a velocità n · 64 Kb/s, ed in tal caso si parla di

collegamento strutturato partizionato (G.704). L'apparecchiatura di interfaccia (convertitore G.704/V.35) è programmabile per estrarre dalla trama E1 (T1) i canali destinati all'utente il quale può, per esempio, collegarsi ad essa mediante un'interfaccia V.35 a 256 Kb/s.

La figura 12.23 mostra una schematizzazione delle gerarchie plesiocrone e sincrone, europee e nord-americane. Sono evidenziate le trame multiple di ordine superiore della gerarchia plesiocrona che sono T3 negli USA ed E3 ed E4 in Europa. Inoltre sono evidenziati i possibili incapsulamenti di trame plesiocrone in trame sincrone.

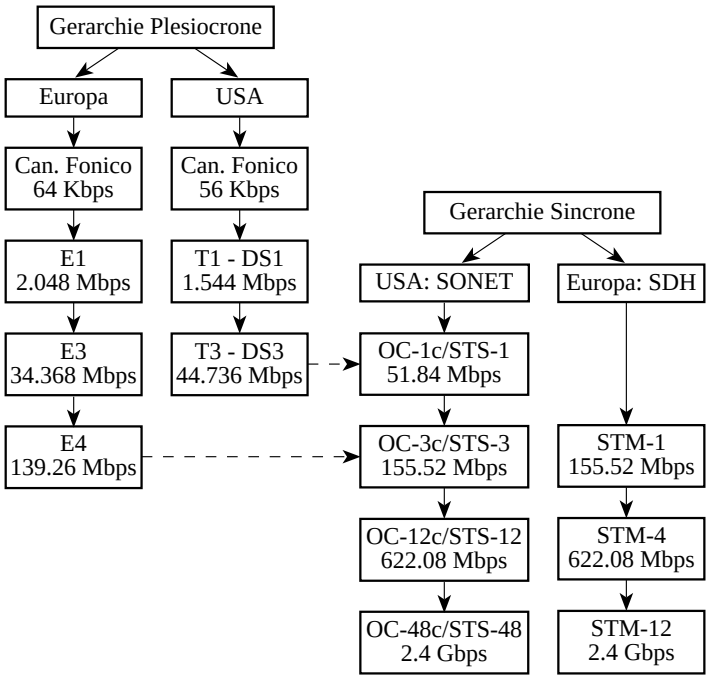


Fig. 12.23 - Gerarchie plesiocrone e sincrone.

I limiti principali delle gerarchie PDH possono essere così riassunti:

- mancata unificazione a livello mondiale: esistono due gerarchie (europea e nord-americana) tra loro incompatibili;
- *pulse stuffing*: la relazione di fase tra i diversi canali tributari in una trama multipla è casuale e variabile nel tempo e questo impedisce di inserire od estrarre facilmente un canale tributario se non ricorrendo ad una operazione di demultiplazione completa della trama multipla seguita da una multiplazione dei nuovi tributari;

- topologico: le gerarchie plesiocrone prevedono solo collegamenti di tipo punto-a-punto e questo è collegato alle limitazioni del punto precedente;
- formati di trame diversi per i diversi ordini gerarchici: non esiste un modo standard per ottenere a partire da una trama quella di ordine superiore;
- overhead limitato: nella trama esiste una capacità di trasportare canali ausiliari estremamente limitata che non consente un controllo adeguato della rete in servizio.

12.6 SDH (SYNCHRONOUS DIGITAL HIERARCHY)

Per superare i limiti presenti in PDH è stata introdotta la gerarchia SDH che è unificata a livello mondiale anche se negli USA si chiama SONET e ha anche una velocità di 51.84 Mb/s non presente altrove. I vantaggi principali di SDH/SONET (detto nel seguito per brevità SDH) sono:

- L'utilizzo di una multiplazione sincrona che permette di inserire flussi a bassa velocità (ad esempio 2 Mb/s) in flussi ad elevata velocità (ad es. 2.4 Gb/s) senza dover effettuare una demultiplazione e una multiplazione completa; analogamente è possibile l'estrazione diretta di un flusso a bassa velocità da uno ad alta. Gli apparati in grado di effettuare queste operazioni sone detti *add/drop multiplexer*.
- La possibilità di trasportare trame PDH all'interno di trame SDH: nella gerarchia europea si inserisce un flusso E4 (140 Mb/s) all'interno di un flusso STS-3 (155 Mb/s), in quella USA si inserisce un flusso T3 (45 Mb/s) all'interno di un flusso STS-1 (51.84 Mb/s), come mostrato in figura 12.23.
- Una topologia di rete ad anello su cui possono essere connessi vari tipi di apparati previsti dallo standard.
- Facilità di gestione: SDH prevede un controllo continuo del tasso di errore e l'integrazione di vari canali ausiliari nelle trame; le procedure di gestione, amministrazione, manutenzione e configurazione, sono a loro volta standardizzate.
- Ambiente multivendor: lo standard SDH consente di ottenere tutti i vantaggi precedenti in una rete formata dall'interconnessione di apparati di costruttori diversi.

L'elemento base di multiplazione SDH è una trama che ha un periodo fondamentale di ripetizione pari a 125 μs (lo stesso di PDH e della trama PCM per motivi di compatibilità). La struttura di questo frame, che è denominata *Synchronous Transport*

Signal at level 1 (STS-1), è rappresentata in figura 12.24. STS-1 è costituito da 6480 bit che trasmessi in 125 μs corrispondono ad un bit rate di 51.84 Mb/s.

L'informazione è organizzata in byte e suddivisa in 9 righe da 90 byte ciascuna, di cui i primi 3 byte costituiscono un overhead di informazioni di controllo mentre il payload è costituito dai successivi 87 byte. I byte sono trasmessi una riga alla volta partendo dal punto indicato con 0 μs.

Lo schema generale di una connessione SDH tra due terminali (*path*) è riportato in figura 12.25. Vengono evidenziati gli add/drop multiplexer che suddividono il path in una o più linee (*line*) e i ripetitori che suddividono una linea in una o più sezioni (*section*).

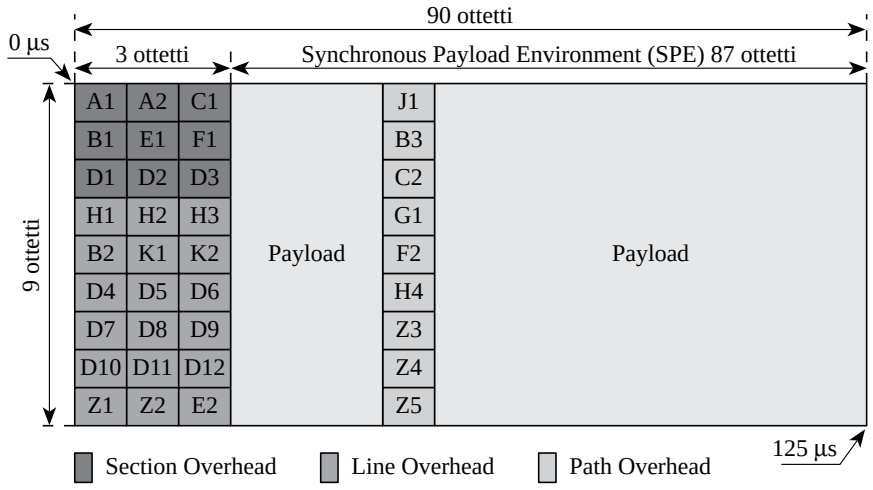


Fig. 12.24 - Formato della trama STS-1.

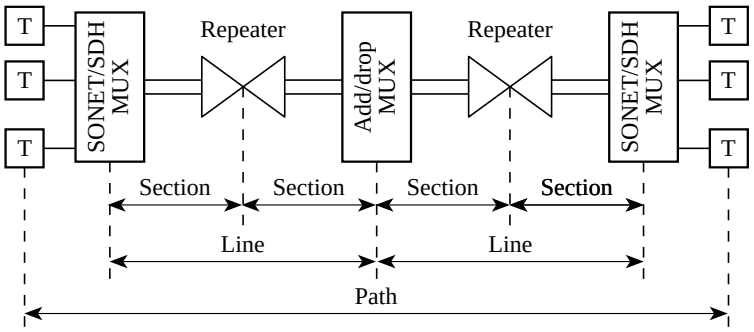


Fig. 12.25 - Gerarchia fisica.

Alla gerarchia fisica di figura 12.25 è associata la gerarchia logica (stratificazione dei protocolli) di figura 12.26.

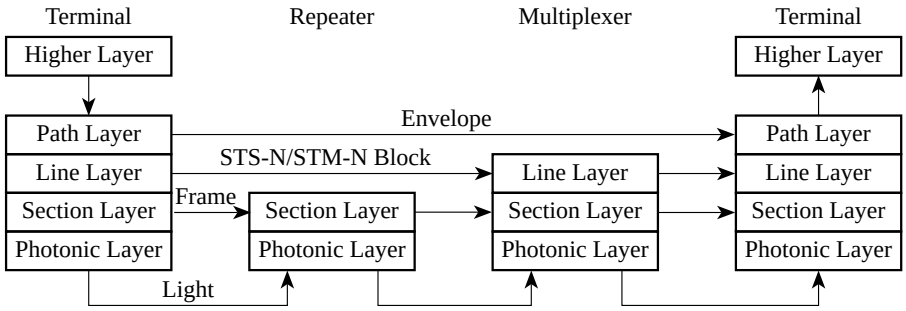


Fig. 12.26 - Gerarchia logica.

Si noti che in SDH non esiste un imbustamento classico con una trama formata da un header e un payload, ma piuttosto ogni livello (path, line, section) ha un overhead predefinito nella trama SDH. All'interno della sezione di overhead trovano posto le seguenti informazioni:

- alcuni byte di framing che servono per determinare l'inizio della trama STS-1;
- i puntatori alle trame dei vari canali multiplati;
- il numero di canali trasportati da un frame per determinare quali sono i puntatori validi;
- informazioni di *Operation And Maintenance* (OAM) che consentono la supervisione e la manutenzione del sistema.

La tabella 12.10 riporta le velocità attualmente definite per SDH e per SONET e le sigle usate per identificarle.

SONET	SDH	Data Rate (Mb/s)
STS-1	STM-0	51.84
STS-3	STM-1	155.52
STS-9	STM-3	466.52
STS-12	STM-4	622.08
STS-18	STM-6	933.12
STS-24	STM-8	1244.16
STS-36	STM-12	1866.24
STS-48	STM-16	2488.32

Tab. 12.10 - Velocità SDH/SONET.

La prima struttura di trama europea è denominata *Synchronous Transport Module at level 1* (STM-1), ed è rappresentata in figura 12.27. STM-1 è costituito da 19440 bit che trasmessi in 0.125 ms corrispondono ad un bit rate di 155.52 Mb/s. L'informazione è organizzata in byte e suddivisa in 9 righe da 270 byte ciascuna, di cui i primi 9 byte costituiscono un overhead di informazioni di controllo, mentre il payload è costituito dai successivi 261 byte. Si noti come questi valori siano tutti esattamente il triplo dei valori riportati per la trama STS-1 in figura 12.24.

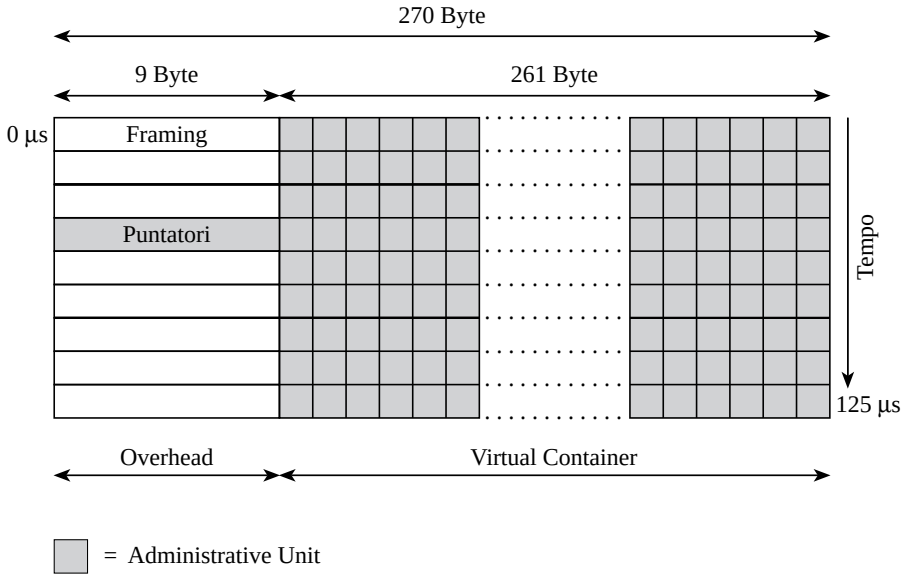


Fig. 12.27 - Struttura della trama STM-1 di SDH.

La sezione utile al trasporto dei dati ha una capacità di 261 x 9 = 2349 ottetti trasmessi in 0.125 ms equivalenti a circa 150 Mb/s e viene chiamata *Virtual Container* (VC). Questo nome è dovuto al fatto che SDH può trasportare tutti i tipi di trama appartenenti a qualunque gerarchia di multiplazione esistente fino ad un intero canale E4 (140 Mb/s). L'insieme costituito da un Virtual Container e dai relativi puntatori prende il nome di *Administrative Unit* (AU).

Le trame dei vari canali da multiplare in STM-1 (payload) possono giungere al multiplexer non allineate nel tempo né tra loro né tanto meno con il Virtual Container. Per risolvere questo problema il multiplexer SDH determina dove inizia la trama di ogni canale e inserisce questa informazione in un *puntatore* della sezione di overhead.

Inoltre, non essendo il payload allineato al Virtual Container, può essere necessario posizionarlo su due trame successive, come mostrato in figura 12.28.

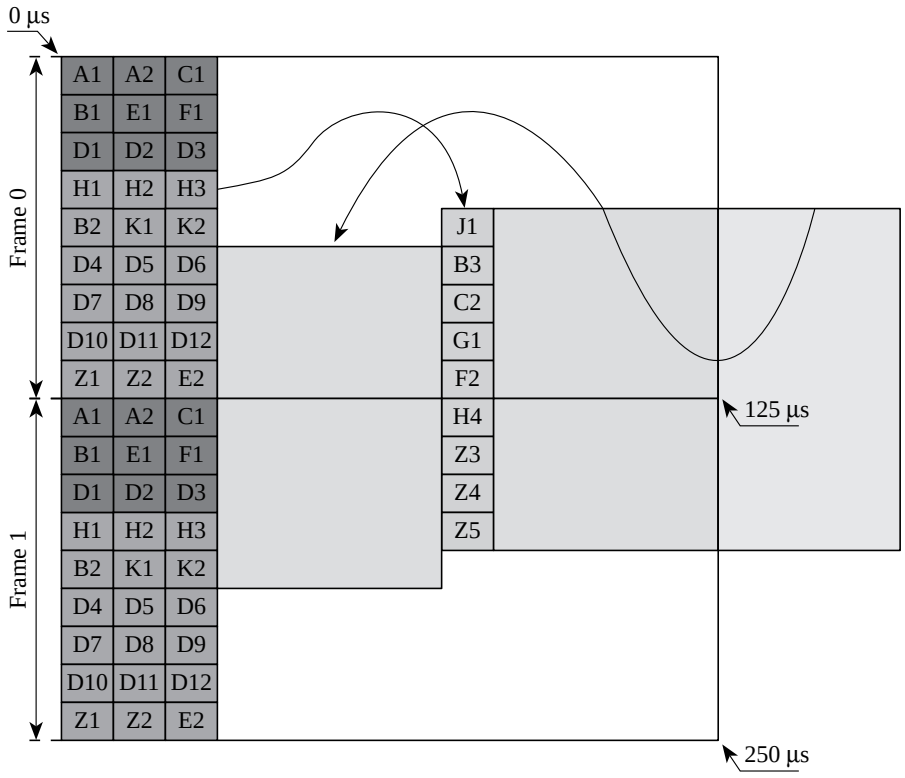


Fig. 12.28 - Posizionamento di un virtual container su due trame.

Il livello successivo della gerarchia sincrona è il *Synchronous Transport Module at level 4* (STM-4) che ha una capacità di 622 Mb/s, quattro volte superiore a quella di STM-1, pur mantenendo lo stesso periodo di ripetizione di 0.125 ms (figura 12.29).

L'algoritmo di costruzione di una trama di gerarchia superiore a partire da *N* trame di gerarchia inferiore si basa sull'interleaving dei singoli byte. Ad esempio, la figura 12.30 mostra come tre trame STS-1 (STS-1(a), STS-1(b) e STS-1(c)) possano essere raggruppate in una trama STS-3. Si noti che i byte della trama STS-3 hanno una durata pari a un terzo di quelli della trama STS-1. L'interleaving può essere meglio compreso analizzando la posizione assunta nella trama STS-3 dai byte a, b, c, d, e, f, g, h, i, l, m e n.

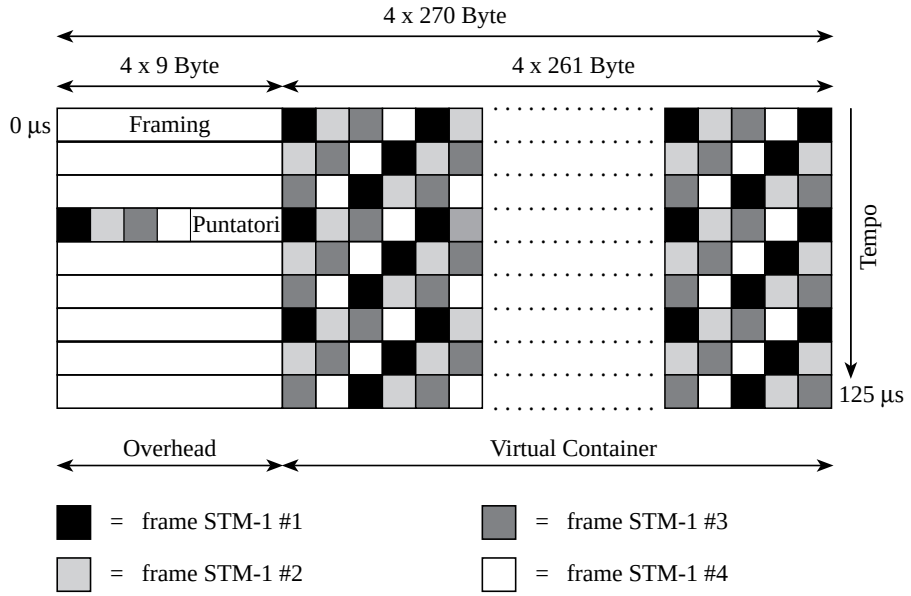


Fig. 12.29 - Struttura della trama STM-4 di SDH.

Al livello gerarchico successivo la trama STM-16, dotata di una capacità pari a 2.4 Gb/s, viene costruita intercalando quattro trame di livello 4 in un'unica trama di livello 16.

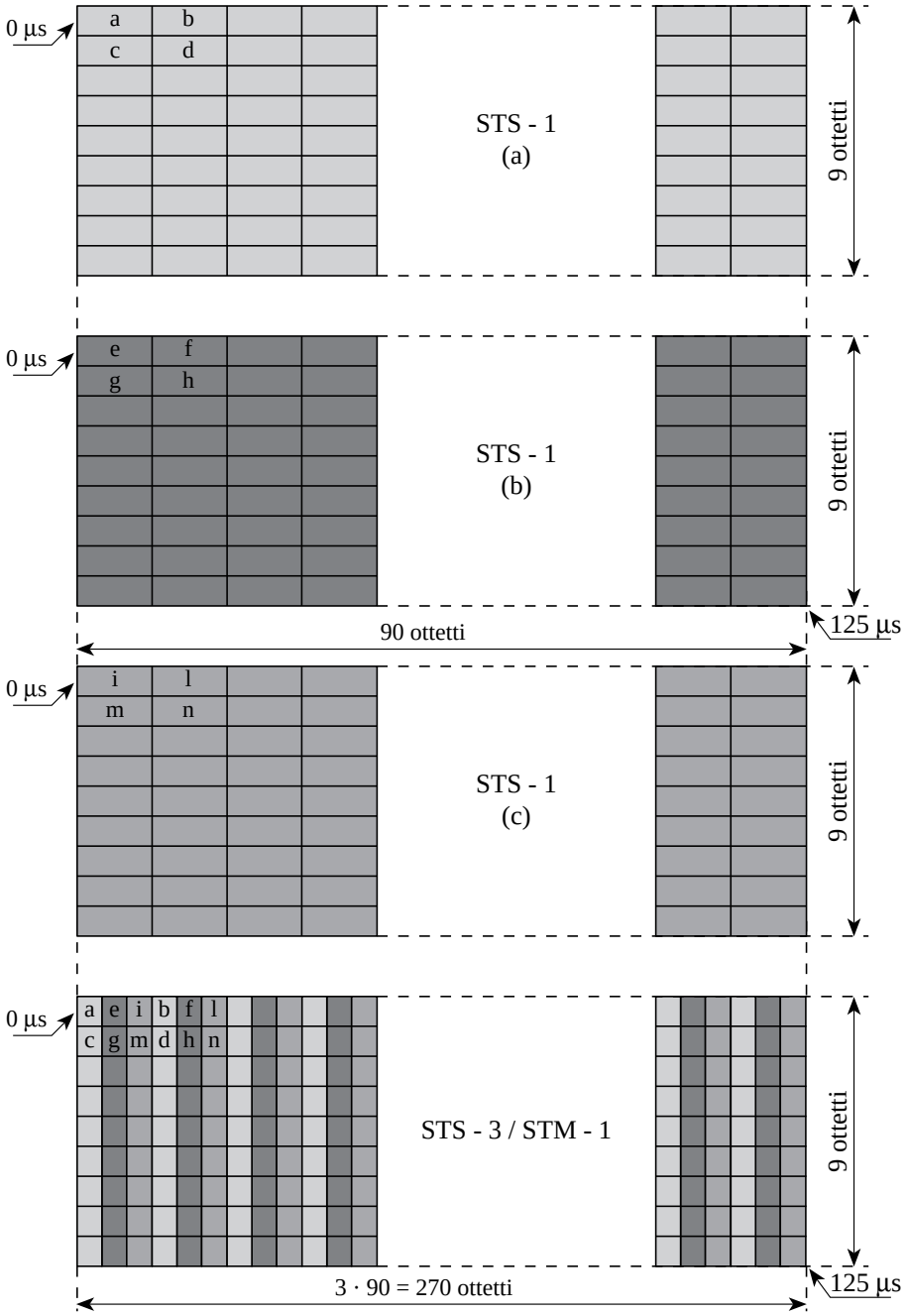


Fig. 12.30 - Raggruppamento di tre trame STS-1 in una trama STS-3.

12.7 ISDN

ISDN (*Integrated Services Digital Network*) rappresenta l'evoluzione delle reti commutate pubbliche analogiche. Basata sulla tecnologia digitale, offre l'integrazione di servizi di elevata qualità (telefonia digitale, trasmissione dati, telecontrolli e teleallarmi, fax G4, ecc.) attraverso un ridotto numero di interfacce standard. Trattandosi di uno standard internazionale per rete digitale commutata, è possibile collegarsi e usufruire di questi servizi con qualsiasi utente della rete.

Inoltre, una delle funzionalità più interessanti di ISDN è l'identificazione dell'utente chiamante, che permette di automatizzare numerose procedure di accesso a servizi informatici e fornisce maggiori possibilità di controllo dal punto di vista della sicurezza rispetto alle attuali linee analogiche.

12.7.1 Architettura della rete ISDN

La rete ISDN prevede due tipi di accesso: l'accesso base, principalmente concepito per l'utente finale, e l'accesso primario, destinato a centri a loro volta erogatori di servizi, quale un centralino telefonico privato.

Accesso base

L'accesso base (o "2 B + D") consiste in due canali a 64 Kb/s (detti canali B) e in un canale dati di servizio a 16 Kb/s (detto canale D). La struttura dell'accesso base è riportata in figura 12.31.

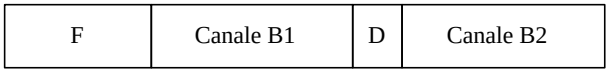


Fig. 12.31 - Struttura dell'accesso base ISDN.

L'accesso base prevede una velocità di trasmissione di 192 Kb/s, di cui 144 utilizzati per i 2 canali B e il canale D, e i restanti 48 per informazioni di controllo e di sincronismo.

Disponendo di due canali telefonici digitali, l'accesso base permette di attivare contemporaneamente due comunicazioni telefoniche, oppure di effettuare un trasferimento dati o inviare un fax durante una telefonata, o di inviare su un canale la voce e sull'altro immagini video compresse (videotelefono).

I dati trasmessi sul canale D sono codificati secondo il formato LAPD (Link Access Protocol D-channel) definito dalla raccomandazione CCITT Q.921, con

formato di trama identico all'HDLC, ma diversa struttura dei campi di indirizzo (si veda il paragrafo 13.5.3).

Accesso primario

Per il collegamento ad utenze particolari, quali i centralini privati (PABX: Private Automated Branch Exchange), è previsto un altro tipo di accesso, detto accesso primario o "30 B + D" (in Europa). Si tratta di un accesso a 1.544 Mb/s negli Stati Uniti (23 canali B più un canale D) e a 2 Mb/s in Europa (30 canali B più un canale D).

Da un accesso primario è anche possibile estrarre canali multipli del canale base B, i cosiddetti canali H. Per esempio, il canale H0 è formato da 6 canali B e fornisce una velocità di 384 Kb/s.

12.7.2 Interfacce

ISDN si basa sul principio di definire una serie di punti di riferimento per i diversi tipi di terminali dell'utente. La relazione tra punti di riferimento e interfacce è schematizzata in figura 12.32.

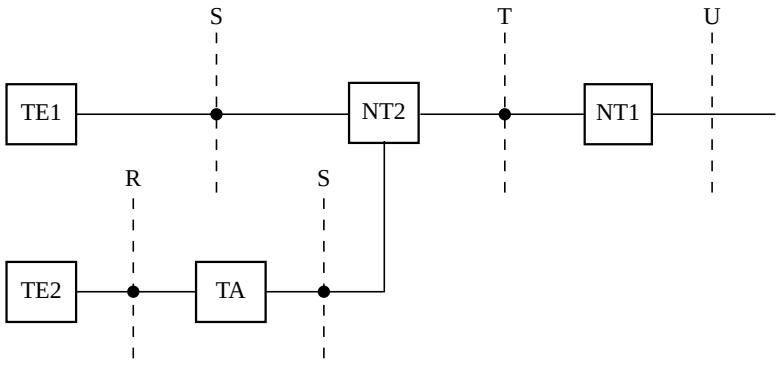


Fig. 12.32 - Modello di riferimento per le interfacce ISDN.

TE1 è un terminale con interfaccia di rete standard ISDN (detta di tipo 'S') per accesso base o primario, in full-duplex. TE2 è un terminale con interfaccia non ISDN (detta di tipo 'R', per esempio una RS-232), e TA è un Terminal Adapter che converte l'interfaccia non ISDN in interfaccia di tipo 'S'. NT1 (Network Terminator 1) è il punto di riferimento equivalente al livello 1 del modello OSI per ISDN.

L'interfaccia di tipo 'T' rappresenta il punto in cui il fornitore di servizio dà l'accesso ISDN alle apparecchiature dell'utente. NT2 (Network Terminator 2) rappresenta i dispositivi che operano nell'ambito dei primi tre livelli OSI, comprendendo quindi commutazione, impacchettamento dei dati, ecc. Spesso, soprattutto nei paesi in cui vige un regime di monopolio, le apparecchiature NT1 e NT2 sono fuse insieme, per esempio all'interno di un centralino telefonico ISDN.

BIBLIOGRAFIA

[1] J. E. McNamara, "Techical Aspects of Data Communication", third edition, Digital Press, Bedford (MA), USA, 1988.

[2] G. Held, "Data Communication Networking Devices", Wiley, third edition, 1992.

[3] C. G. Omidyar, A. Aldridge: "Introduction to SDH/SONET", IEEE Communications Magazine, September 1993

[4] William Stalling, "ISDN and Broadband ISDN", MacMillam Publishing Company, New York, 1992.

13

I PROTOCOLLI DI LINEA ED I SERVIZI A PACCHETTO

13.1 INTRODUZIONE

Questo capitolo tratta due differenti tematiche - i protocolli di linea e i servizi a commutazione di pacchetto - nell'ottica del loro utilizzo come mezzi di interconnessione di bridge, router e gateway, per realizzare un internetworking multiprotocollo.

I protocolli di linea sono i protocolli di livello 2 (Data Link) che vengono utilizzati sulle linee pubbliche per trasmissione dati. Nell'ambito delle problematiche di internetworking ci si concentra sui protocolli per linee di tipo punto-punto. I protocolli di linea oggi usati sono tutti discendenti di SDLC (*Synchronous Data Link Control*), protocollo introdotto da IBM con l'architettura SNA.

Tali protocolli formano una famiglia i cui componenti più importanti sono HDLC (*High Level Data Link Control*), LAPB (*Link Access Procedure Balanced*), LAPD (*Link Access Procedure D-channel*), LAPF (*Link Access Procedure to Frame mode bearer services*) e LLC (*Logical Link Control*, già descritto nel paragrafo 5.7).

I servizi a commutazione di pacchetto sono quei servizi che vengono offerti dalle reti geografiche, pubbliche o private, a commutazione di pacchetto. Tra questi vengono trattati X.25, Frame Relay e SMDS.

Una tabella comparativa chiude il capitolo.

13.2 HDLC, LAPB E SDLC

Si tratta di protocolli di linea (livello 2 del modello OSI) progettati per canali geografici di tipo punto-punto o multipunto.

Lo standard OSI prevede esplicitamente l'adozione di HDLC (High Level Data Link Control) il cui funzionamento è descritto dettagliatamente negli standard riportati in bibliografia. Gli altri protocolli sono varianti di HDLC e quanto detto nel resto del paragrafo è valido per HDLC, quando non diversamente specificato.

Originariamente HDLC era in grado di funzionare solo su linee sincrone, ma con lo standard ISO 3309 è stato esteso anche alle linee asincrone.

13.2.1 Connessioni

Il protocollo HDLC connette due o più stazioni. La connessione può essere bilanciata *(balanced)* o sbilanciata *(unbalanced).*

In una connessione bilanciata il numero di stazioni è limitato a due (connessione punto-punto), le stazioni sono paritetiche *(combined stations)* e il protocollo è full-duplex, cioè ogni stazione può trasmettere quando ne ha necessità, indipendentemente da ciò che sta facendo l'altra stazione.

In una connessione sbilanciata esiste una stazione primaria e le altre stazioni (che possono essere molte) sono secondarie. La trasmissione avviene in modalità half-duplex, con la stazione primaria che opera come master del canale multi-punto e le secondarie come slave.

Sulle connessioni sbilanciate i messaggi inviati dalla stazione primaria sono detti comandi *(command),* mentre i messaggi delle stazioni secondarie sono detti risposte *(response).*

Sulle connessioni bilanciate ognuna delle due stazioni può generare una trasmissione, cioè inviare un comando e l'altra, conseguentemente, dovrà generare una risposta.

13.2.2 NRM (Normal Reponse Mode)

Il *Normal Response Mode* è una delle modalità operative previste da HDLC ed è l'unica modalità operativa prevista da SDLC. Si tratta di una connessione sbilanciata half-duplex in cui una stazione secondaria non può iniziare una trasmissione se non riceve una autorizzazione esplicita dalla stazione primaria. In questa modalità possono esserci molte stazioni secondarie che vengono ciclicamente autorizzate dalla stazione primaria a trasmettere su un canale punto-multipunto.

13.2.3 ABM (Asynchronous Balanced Mode)

L'*Asynchronous Balanced Mode* è una modalità operativa prevista da HDLC ed è anche l'unica modalità operativa prevista da LAPB. Si tratta di una connessione bilanciata full-duplex tra due combined station. Entrambe le stazioni possono iniziare a trasmettere quando ne hanno necessità e la trasmissione nei due sensi può avvenire in parallelo.

13.2.4 ARM (Asynchronous Response Mode)

L'*Asynchronous Response Mode* è una modalità operativa prevista da HDLC simile a NRM, ma limitata a due stazioni. In presenza di tale limite la stazione secondaria può iniziare una trasmissione senza l'autorizzazione della stazione primaria, che però continua a mantenere la responsabilità della gestione del collegamento.

13.2.5 Bit stuffing

La trama è delimitata da due caratteri flag che corrispondono alla configurazione binaria 01111110 e che marcano univocamente l'inizio e la fine di una trama, oppure la separazione tra due trame successive.

Perché il flag risulti un marcatore univoco, HDLC usa la tecnica del bit stuffing che garantisce che solo il carattere flag contenga sei uno consecutivi. Infatti il bit stuffing analizza la trama (flag esclusi) prima di trasmetterla e inserisce un bit a zero dopo cinque uni consecutivi (indipendentemente dal valore del bit successivo).

Il ricevitore, se riceve una sequenza di cinque uni e uno zero, elimina lo zero che era stato inserito dal *bit stuffing*, se riceve sei uni e uno zero identifica il carattere flag.

13.2.6 Formato della trama HDLC

Il formato della trama HDLC è riportato in figura 13.1.

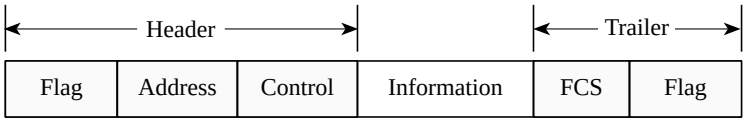


Fig. 13.1 - Trama HDLC.

La trama è composta da tre parti principali: un header, un campo information a lunghezza variabile e un trailer.

Il campo *address* è lungo un ottetto e ha il significato di indirizzo della stazione. Concepito originariamente per il NRM di SDLC, il campo address non ha motivo di esistere negli altri modi di HDLC (ABM e ARM), se non per ragioni di compatibilità di formato.

Nel modo NRM il campo address contiene l'indirizzo della stazione ricevente, nel caso di un messaggio di command, e l'indirizzo della stazione trasmittente, nel caso di un messaggio di response.

Il campo *control* è un campo estremamente importante e può essere lungo uno o due ottetti. Esso assume i tre formati mostrati in figura 13.2.

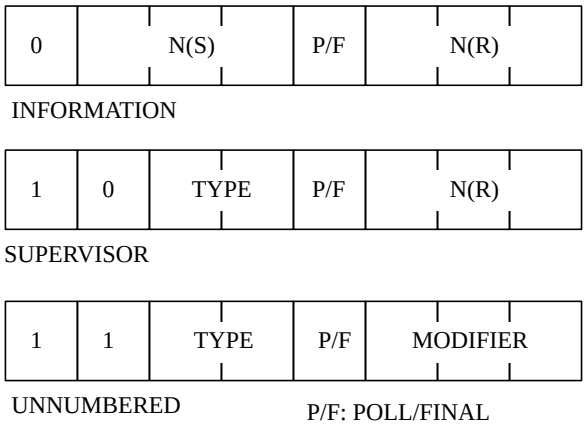


Fig. 13.2 - Formati del campo control.

Il formato *information* è usato per le trame che trasportano i dati in modalità connessa e ha anche la possibilità di trasportare un acknowledge (ACK) per la trasmissione nella direzione inversa (tecnica detta di *piggybacking*). Le trame di questo formato sono dette *I-frame*.

Il formato *supervisor* non prevede la presenza del campo information nella trama ed è usato per trasportare informazioni di controllo relative agli I-frame; ad esempio, fornire un ACK in assenza di traffico nella direzione inversa, operare il controllo di flusso, ecc. Le trame di questo formato sono dette *S-frame*.

Il formato *unnumbered* è utilizzato per due scopi diversi: trasportare dati di utente in modalità non connessa e trasportare messaggi di controllo del collegamento (inizializzazione, diagnostica, ecc.). Le trame di questo formato sono dette U-frame.

La modalità operativa più comune del protocollo HDLC è quella connessa in cui il protocollo scambia I-frame, anche se la modalità non connessa può essere utilizzata tramite gli *U-frame*.

Nella modalità connessa è necessario numerare le trame. HDLC prevede due possibili numerazioni alternative: la normale impiega un numero di trama su tre bit (modulo 8), mentre la estesa (Extended) impiega un numero di trama su 7 bit (modulo 128).

I sottocampi N(S) e N(R) del campo control sono destinati ad ospitare i numeri di trama. Quando si opera in modalità normale (modulo 8) il campo control è sempre lungo 8 bit (1 ottetto), poiché N(S) e N(R) sono lunghi 3 bit ciascuno. Quando invece si opera in modalità estesa (modulo 128), N(S) e N(R) sono lunghi 7 bit e quindi il campo control è lungo un ottetto nel caso degli U-frame, due ottetti nel caso degli I-frame e degli S-frame.

13.2.7 U-frame

I diversi tipi di U-frame, distinguibili in funzione dei valori assunti dai sottocampi *type* e *modifier* del campo control, sono di seguito elencati.

- *SABM (Set Asynchronous Balanced Mode).* È una trama di comando utilizzata per inizializzare una connessione ABM con numeri di sequenza su tre bit (modulo 8); il campo control è sempre su un ottetto.
- *SABME (Set Asynchronous Balanced Mode Extended).* È una trama di comando utilizzata per inizializzare una connessione ABM con numeri di sequenza su sette bit (modulo 128); il campo control delle trame I e S è su due ottetti.
- *SNRM (Set Normal Response Mode).* È una trama di comando utilizzata per inizializzare una connessione NRM con numeri di sequenza su tre bit (modulo 8); il campo control è sempre su un ottetto.
- *SNRME (Set Normal Response Mode Extended).* È una trama di comando utilizzata per inizializzare una connessione NRM con numeri di sequenza su sette bit (modulo 128); il campo control delle trame I e S è su due ottetti.
- *UI (Unnumbered Information).* È una trama utilizzata per inviare dati di utente in modalità non connessa. È molto utilizzata dalla variante di HDLC, detta LLC, che opera sulle reti locali (si veda il paragrafo 5.7.2).
- *DISC (DISConnect).* È una trama di comando utilizzata per terminare una connessione.
- *XID (eXchange station IDentification).* È una trama di comando o di risposta usata per scambiare e negoziare parametri tra le stazioni, ad esempio l'utilizzo di una FCS su 16 o 32 bit.

- *UA (Unnumbered Acknowledge).* È una trama di risposta usata come acknowledge della ricezione di un messaggio SABM, SABME, SNRM, SNRME o DISC.
- *FRMR (FRaMe Reject).* È una trama di risposta usata per indicare la ricezione di un messaggio con FCS corretta, ma che non può essere accettato per una qualche altra ragione, ad esempio una stazione SDLC che riceva un SABM invia un FRMR, non potendo attivare il modo ABM.
- *DM (Disconnect Mode).* È una trama di risposta usata come acknowledge della ricezione di un messaggio DISC.

13.2.8 S-frame

Gli S-frame sono usati in associazione agli I-frame nella modalità connessa. Il sottocampo *N(R)* del campo control contiene il numero di sequenza del prossimo frame che la stazione si aspetta di ricevere; questo serve anche da ACK per tutti i frame con numero di sequenza minore di N(R).

Sono previsti quattro tipi di S-frame, distinguibili in funzione dei valori assunti dal sottocampo *type* del campo control, di seguito elencati.

- *RR (Receiver Ready).* È un frame utilizzato per fornire un ACK in assenza di traffico (in presenza di traffico l'ACK viene inviato tramite piggybacking in un I-frame), oppure per indicare che la stazione è pronta a ricevere nuovi I-frame, se precedentemente era stato inviato un S-frame di tipo RNR.
- *RNR (Receiver Not Ready).* È un frame utilizzato per indicare che la stazione è temporaneamente impossibilitata a ricevere nuovi I-frame.
- *REJ (REJect).* È un frame utilizzato per chiedere la ritrasmissione di tutti gli I-frame già inviati a partire da quello con numero di sequenza pari a N(R).
- *SREJ (Selective REJect).* È un frame utilizzato per chiedere la ritrasmissione del solo I-frame con numero di sequenza pari a N(R). Questo messaggio è supportato unicamente da HDLC e non da LAPB.

13.2.9 I-frame

Gli I-frame sono di un solo tipo e trasportano i dati di utente. Il sottocampo *N(S)* del campo control contiene il numero di sequenza che identifica l'I-frame. Il sottocampo *N(R)* del campo control contiene un ACK piggybacked per gli I-frame che viaggiano in direzione opposta.

13.2.10 Il bit P/F

Il bit P/F *(Poll/Final)* ha due significati diversi nei modi bilanciati e sbilanciati.

Nei modi sbilanciati è messo a uno dalla stazione primaria per invitare la stazione secondaria a trasmettere (poll). La stazione secondaria può trasmettere un gruppo di frame in cui il bit P/F è a zero, ad eccezione dell'ultimo frame che ha P/F a uno (final).

Nel modo bilanciato il bit P/F uguale a uno, in un frame di tipo command, significa che si chiede l'acknowledge di quel frame. La stazione ricevente risponde con il messaggio di response (acknowledge) con il bit P/F a uno.

13.2.11 FCS

Il campo FCS (*Frame Control Sequence*) contiene una CRC che può essere su 16 bit (2 ottetti) o su 32 bit (4 ottetti). La lunghezza della CRC da utilizzarsi viene decisa dalle stazioni tramite messaggi di tipo XID.

13.2.12 Esempio

La figura 13.3 mostra un esempio di comunicazione HDLC di tipo ABM in cui è possibile comprendere il ruolo degli I-frame e degli S-frame, la modalità di numerazione delle trame e il ruolo delle liste di ritrasmissione.

La stazione A inizia a numerare le trame a partire da 0, mentre la stazione B a partire da 3. Il primo I-frame che invia A a B ha quindi N(S) = 0 e N(R) = 3, indicati più sinteticamente nella figura con la notazione I(0,3). Questo significa che la stazione A sta trasmettendo la trama 0 e ha ricevuto con successo dalla stazione B la trama 2 ed attende la trama 3.

Analogamente B trasmette un messaggio di tipo I(3,0), cioè sta trasmettendo la trama 3, con ACK per la trama 7, se le stazioni operano con numerazione modulo 8, oppure per la trama 127 se operano modulo 128.

Il frame I(6,1) inviato da B ad A contiene l'ACK per il frame 0 inviato da A a B e l'indicazione che ora B attende di ricevere il frame 1 da A.

Trasmesso il frame I(7,2), B non ha più informazioni da inviare ad A, ma deve comunque fornire gli ACK per i frame 2, 3, 4, 5 inviati da A a B. Effettua tale operazione tramite due S-frame di tipo RR (*Receiver Ready*). Con lo S-frame RR(5) fornisce ad A l'ACK per i frame 2, 3 e 4, mentre con RR(6) fornisce l'ACK per il frame 5 e comunica ad A di essere pronto ad accettare il frame 6.

Si noti che quando arriva l'ACK per un frame, questo viene tolto dalla lista di ritrasmissione.

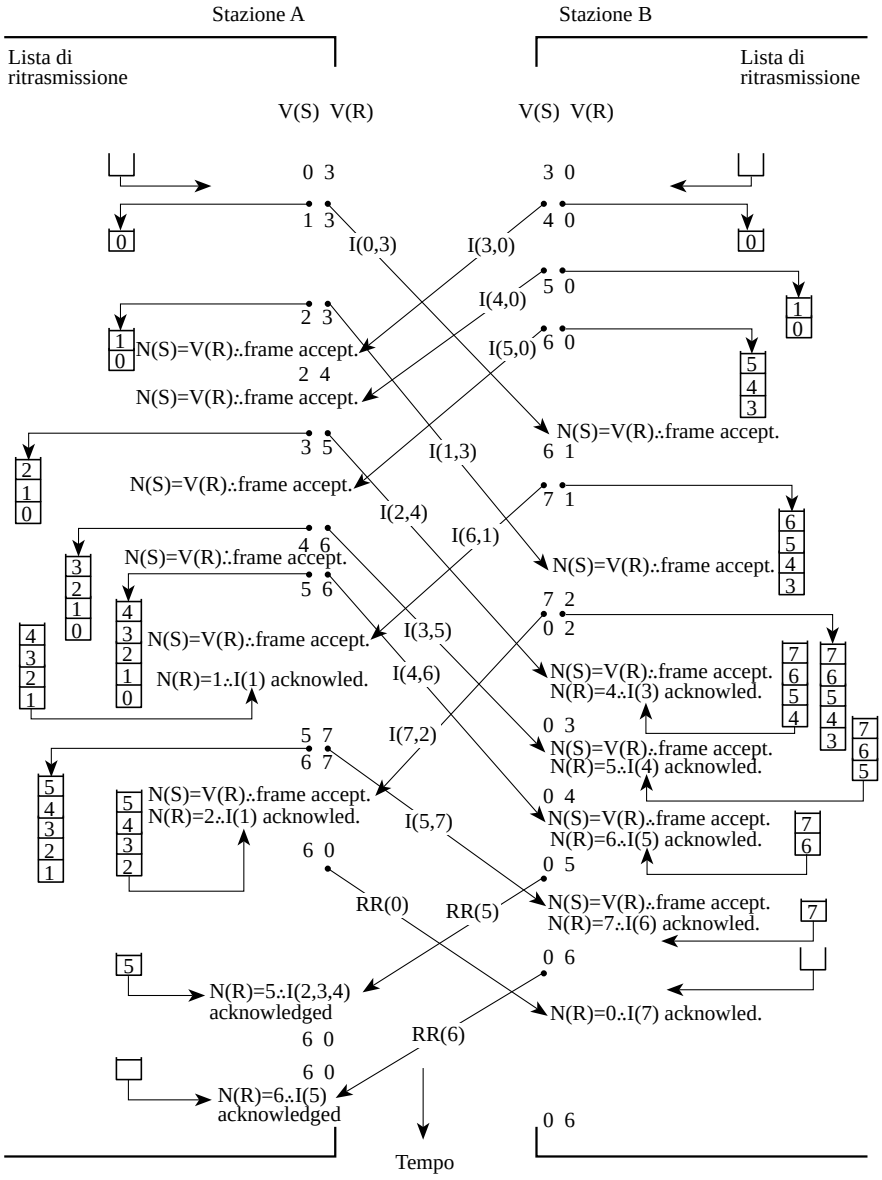


Fig. 13.3 - Esempio di comunicazione in HDLC.

13.3 PPP

13.3.1 Introduzione

Il protocollo HDLC ha una grave carenza: non ha una modalità standard per trasmettere sullo stesso canale pacchetti generati da diversi protocolli di livello superiore. Per questo motivo la comunità di Internet ha introdotto nel luglio 1990 una estensione di HDLC, basata sullo standard HDLC ISO 4335, detta PPP *(Point-to-Point Protocol).* Tale estensione è stata documentata in vari RFC (si veda il paragrafo 16.1) il più recente dei quali è lo RFC 1548 del settembre 1993.

13.3.2 Il livello Data Link

Il formato del pacchetto PPP è mostrato in figura 13.4.

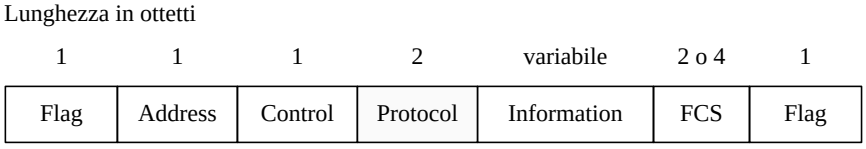


Fig. 13.4 - Formato della trama PPP.

La differenza principale rispetto ad HDLC risiede nella presenza di un campo *protocol* lungo 2 ottetti. Tale campo contiene la codifica del protocollo di livello superiore la cui PDU è contenuta nel campo information. L'appendice A, paragrafo A.8, riporta un elenco dei possibili valori che può assumere il campo protocol.

Si noti inoltre che PPP pone limitazioni ai valori leciti per alcuni altri campi e in particolare:

- Il campo *address* deve sempre contenere la sequenza binaria 11111111 che corrisponde alla codifica broadcast. PPP non assegna indirizzi alle stazioni essendo un protocollo punto-punto.
- Il campo *control* deve sempre contenere la sequenza 11000000, cioè la trama deve essere un U-frame di tipo UI (Unnumbered Information). La lunghezza del campo control è quindi sempre pari a un ottetto e la trasmissione è di tipo non connesso.
- Il campo *information* ha una lunghezza compresa tra 0 e 1500 ottetti. La lunghezza massima può essere modificata di comune accordo dalle stazioni.

- Il campo FCS ha una lunghezza di 2 ottetti, ma può essere portata a 4 ottetti di comune accordo dalle stazioni.

PPP fornisce un metodo standard per trasmettere pacchetti provenienti da più protocolli diversi, sullo stesso collegamento seriale sincrono o asincrono. Per raggiungere tale scopo, PPP utilizza:

- il protocollo ausiliario LCP *(Link Control Protocol)* per creare, configurare e verificare la connessione a livello Data Link;
- una famiglia di protocolli NCP *(Network Control Protocol)* per configurare i diversi protocolli di livello Network.

13.3.3 Il protocollo LCP

Il Link Control Protocol fornisce un metodo per creare, configurare, gestire e terminare le connessioni punto-punto. LCP è un protocollo estendibile.

LCP opera in quattro fasi:

- apre la connessione e negozia i parametri di configurazione;
- verifica, opzionalmente, la qualità del collegamento per determinare se è sufficiente per i protocolli di livello superiore;
- attiva i protocolli NCP associati ai vari livelli di network affinché svolgano le relative procedure di inizializzazione;
- termina il collegamento.

13.4 X.25

13.4.1 Introduzione

La tecnologia a commutazione di pacchetto X.25 è stata la prima ad essere introdotta ed è ormai disponibile da più di 20 anni. Le reti X.25 sono state definite dal CCITT nel 1976, 1980, 1984 con lo standard intitolato *"Interface between DTE and DCE for Terminal Operating in the Packet Mode and Connected to Public Data Network by Dedicated Circuit"*.

Lo standard definisce quindi l'interfaccia tra un DTE-X.25 (ad esempio un calcolatore o un router) e un DCE-X.25 (ad esempio, un modem), ma non come funziona la rete al suo interno (figura 13.5).

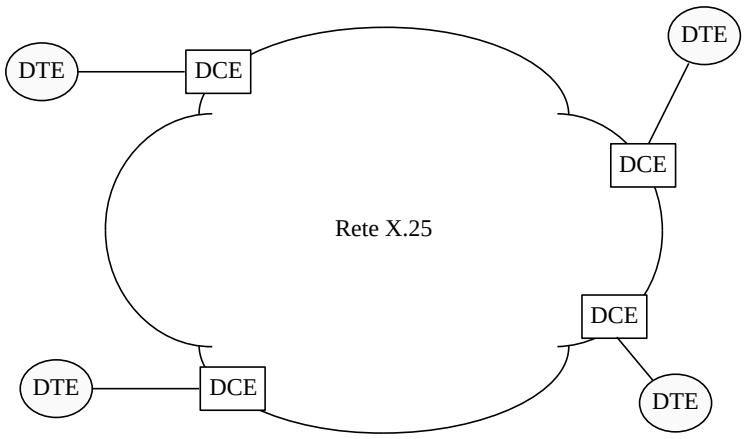


Fig. 13.5 - DTE, DCE e rete X.25.

La rete X.25 è realizzata con dei commutatori di pacchetto (PSE: *Packet Switching Exchange*) cui sono connnessi i DCE secondo lo schema generale mostrato in figura 13.6.

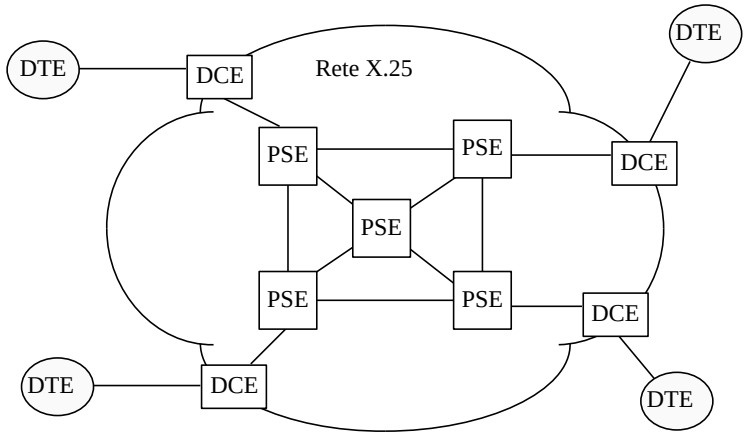


Fig. 13.6 - Struttura interna di una rete X.25.

Tuttavia il termine "rete X.25" rimane in parte non corretto: infatti X.25 non specifica come deve essere organizzata la rete all'interno, ad esempio, con quali criteri si instradano i messaggi tra i PSE.

Lo standard X.25 è stato impiegato con successo per realizzare reti geografiche

sia pubbliche (ad esempio, in Italia, *Itapac*), sia private. Le reti X.25 forniscono servizi di tipo connesso e le connessioni sono dette circuiti virtuali. X.25 prevede sia circuiti virtuali permanenti (PVC: *Permanent Virtual Circuit*), sia circuiti virtuali dinamici (SVC: *Switched Virtual Circuit*).

I PVC sono adatti a chi ha necessità di connettersi frequentemente e per lunghi periodi di tempo con un corrispondente fisso, mentre gli SVC sono adatti a chi deve comunicare con diversi corrispondenti.

Alle reti X.25 possono essere collegati anche DTE asincroni a carattere (tipo TTY, terminali video asincroni, PC con interfaccia asincrona, ecc.) tramite un dispositivo detto PAD (*Packet Assembler/Disassembler*) che si occupa di assemblare/disassemblare i pacchetti per il terminale (figura 13.7).

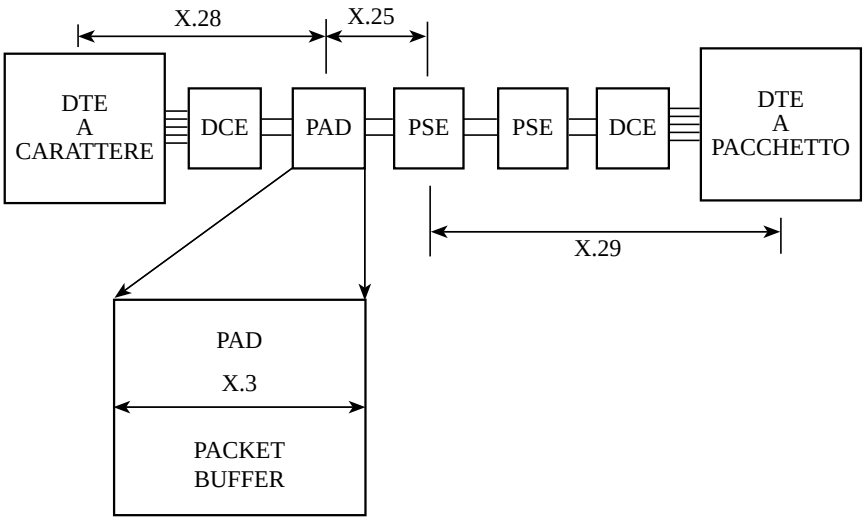


Fig. 13.7 - Relazione tra gli standard X.3, X.25, X.28 e X.29.

Quest'ultima funzionalità è definita dagli standard CCITT X.3, X.28 e X.29, ma riveste scarso interesse per le problematiche di internetworking.

Il vantaggio principale di X.25 è il suo elevato grado di standardizzazione a livello internazionale, il suo limite più spiccato è il basso throughput che si può ottenere, che rende X.25 non troppo idoneo all'internetworking.

Per superare i limiti prestazionali di X.25 sono stati sviluppati altri standard quali Frame Relay e SMDS, che verranno trattati nei paragrafi seguenti.

Lo standard X.25 tratta i primi tre livelli del modello di riferimento OSI.

13.4.2 Il livello Fisico

A livello Fisico le reti X.25 usano linee sincrone punto-punto, con l'unica eccezione della variante X.32 che impiega linee commutate. La velocità delle linee che collegano i DTE varia tipicamente tra 1200 b/s e 64 Kb/s. L'interfaccia di utente è RS-232 per i collegamenti sino a 19200 b/s e V.35 per i collegamenti a velocità maggiore o uguale a 64Kb/s.

13.4.3 Il livello Data Link

A livello Data Link, X.25 adotta il protocollo LAPB (Link Access Procedure Balanced) definito dallo standard ISO 7776 e di derivazione SDLC/HDLC. La connessione viene gestita in ABM (Asynchronous Balanced Mode), cioè in modo full-duplex connesso, con correzione di eventuali errori di trasmissione a livello 2, su ogni tratta.

13.4.4 Il livello Network

Il livello 3 di X.25 è conforme allo standard ISO 8208 e definisce le procedure per la formazione dei circuiti virtuali e per il corretto trasferimento dei dati d'utente. Il pacchetto di livello 3 è imbustato nel campo dati del pacchetto LAPB (figura 13.8).

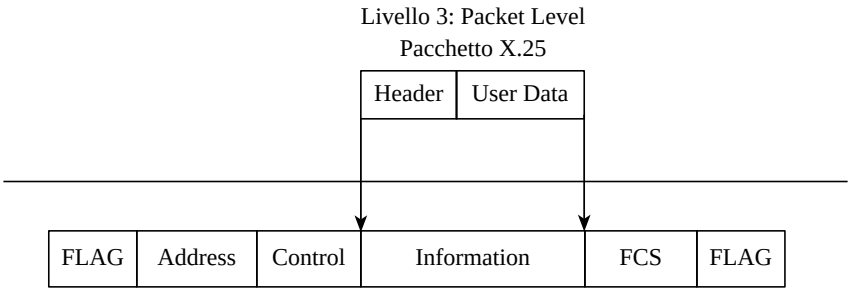


Fig. 13.8 - PDU di livello 2 e 3.

L'header del pacchetto di livello 3 contiene tre campi principali:

- GFI (*General Format Identifier*), di 4 bit, che indica il formato dell'header di livello 3;

- LCI (*Logical Channel Identifier*), di 12 bit, che contiene il numero del circuito virtuale su cui è trasmesso il pacchetto;
- PTI (*Packet Type Identifier*), di 8 bit, che identifica i vari tipi di pacchetto X.25, riportati nella tabella 13.1.

richiesta di chiamata	CAR	chiamata entrante	INC
chiamata completata	CON	chiamata accettata	CAC
richiesta di svincolo	CLR	indicazione di svincolo	CLI
conferma svincolo	CLC	dati	D
interrupt	INT	conferma di interrupt	INTC
pronto a ricevere	RR	non pronto a ricevere	RNR
richiesta di reset	RES	indicazione di reset	REI
conferma di reset	REC	richiesta di restart	RTR
indicazione di restart	RTI	conferma di restart	RTC

Tab. 13.1 - Tipi di pacchetti X.25.

I circuiti virtuali sono identificati tramite lo LCI che, nel caso degli SVC, è assegnato dinamicamente a partire dall'indirizzo di DTE, mentre, nel caso dei PVC, è assegnato permanentemente dal gestore della rete.

L'utilizzo dei vari tipi di pacchetti per richiedere la creazione di un SVC (fase 1), per il suo successivo utilizzo (fase 2) e per la chiusura del SVC stesso (fase 3), è riportato in figura 13.9.

Nell'esempio supporremo che la rete X.25 utilizzata sia Itapac.

Durante la formazione del collegamento (fase 1) un DTE A invia a Itapac un pacchetto CAR (richiesta di chiamata) contenente l'indirizzo del DTE chiamato (DTE B). Itapac invia al DTE B un pacchetto INC (chiamata entrante) per notificargli la richiesta di creazione di un SVC da parte del DTE A.

Il DTE B può rifiutare la chiamata inviando a Itapac un pacchetto CLR oppure accettarla inviando a Itapac un pacchetto CAC (chiamata accettata). In questo secondo caso Itapac conferma al DTE A l'avvenuta connessione tramite un pacchetto CON (avvenuta connessione).

A questo punto inizia la fase di scambio dati (fase 2) che può avvenire contemporaneamente nei due sensi ed utilizza pacchetti di tipo D (data). Se si verificano problemi durante tale fase uno dei due DTE può chiedere il reset del collegamento (pacchetto RES).

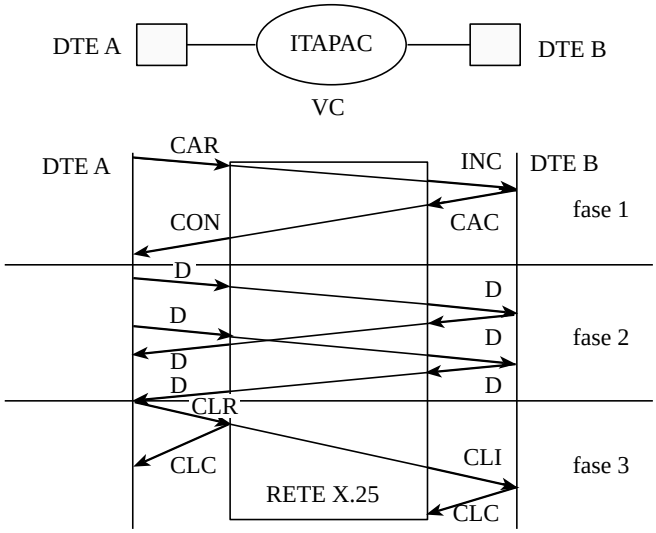


Fig. 13.9 - Esempio di trasferimento dati tramite SVC.

Terminata la fase di scambio dati, si ha l'abbattimento del collegamento (fase 3). Il DTE che vuole chiudere il collegamento invia un pacchetto CLR (richiesta di svincolo) a Itapac, che risponde immediatamente con un pacchetto CLC (conferma di svincolo) e invia al DTE remoto un pacchetto CLI (indicazione di svincolo). Il DTE remoto risponde con CLC (conferma svincolo) a Itapac.

13.4.5 Indirizzamento

Gli indirizzi nelle reti X.25 servono ad attivare gli SVC. Essi sono detti indirizzi di DTE e sono conformi allo standard CCITT X.121.

X.121 propone uno schema di indirizzamento universale (figura 13.10) tramite il quale un DTE può essere individuato tramite un indirizzo internazionale detto *IDN (International Data Number).*

L'IDN è composto da due parti:

- DNIC *(Data Network Identification Code)* che si suddivide ulteriormente in:
  - Country che identifica la nazione,
  - PSN *(Packet Switched Network)* che identifica la rete all'interno della nazione;
- NTN *(Network Terminal Number)* che identifica il DTE all'interno della rete.

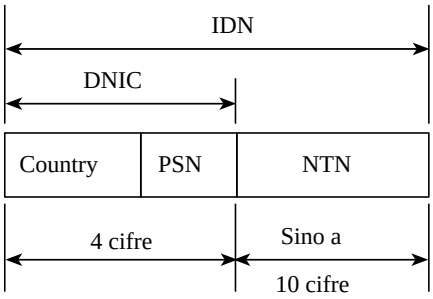


Fig. 13.10 - Formato indirizzo X.121.

A livello nazionale in Itapac ogni utente è identificato da un NUA (*Network User Address*) che è un numero di 8 cifre:

- la prima cifra è sempre 2 e corrisponde alla PSN Itapac;
- le seguenti 1, 2 o 3 cifre sono il prefisso teleselettivo del distretto telefonico, privato dello zero iniziale (es.: 11 per Torino);
- le rimanenti cifre identificano l'utente.

13.4.6 Il campo CUD e il supporto multiprotocollo

Il campo CUD (*Call User Data*) è presente nei pacchetti CAR (*CAll Request*) che servono per attivare uno SVC. Tale campo è utilizzato per permettere a X.25 di fornire un supporto multiprotocollo.

Infatti, anche se X.25 ha un suo livello 3, questo viene normalmente ignorato dalle architetture di rete, che considerano i circuiti virtuali X.25 come collegamenti di livello 2 e quindi non rinunciano al loro livello 3.

Questo implica che quando, ad esempio, un pacchetto TCP/IP transita su una rete X.25 abbia due buste di livello 3, quella di IP e quella di X.25. L'unica eccezione è rappresentata dalle reti OSI (si veda il paragrafo 17.3) che integrano completamente X.25 al loro interno.

In fase di creazione dello SVC si utilizza il campo CUD per identificare a quale architettura di rete appartengono i dati di livello 3 che transitano sullo SVC.

Una tabella dei valori da assegnare al CUD, in funzione del protocollo di livello 3 richiedente, è riportata in appendice A, paragrafo A.10.

13.5 FRAME RELAY

13.5.1 Introduzione

Frame Relay è uno standard che ha delle similitudini con X.25, essendo uno standard di interfaccia DCE-DTE che permette di far convivere diversi circuiti virtuali su una singola linea trasmissiva. Tuttavia le differenze sono altrettanto importanti: Frame Relay è uno standard puramente di livello 2 e quindi differisce da X.25 che ha un suo livello 3; Frame Relay è uno standard pensato per linee trasmissive veloci ed affidabili e quindi non corregge gli errori su ogni tratta trasmissiva come avviene in X.25.

Frame Relay è uno standard appositamente progettato per interconnettere router e bridge remoti in modo efficiente, con prestazioni nettamente superiori a quelle di X.25.

L'architettura di una rete Frame Relay è schematizzata in figura 13.11, dove si evidenzia come una rete Frame Relay sia un mezzo per creare circuiti virtuali tra DTE Frame Relay.

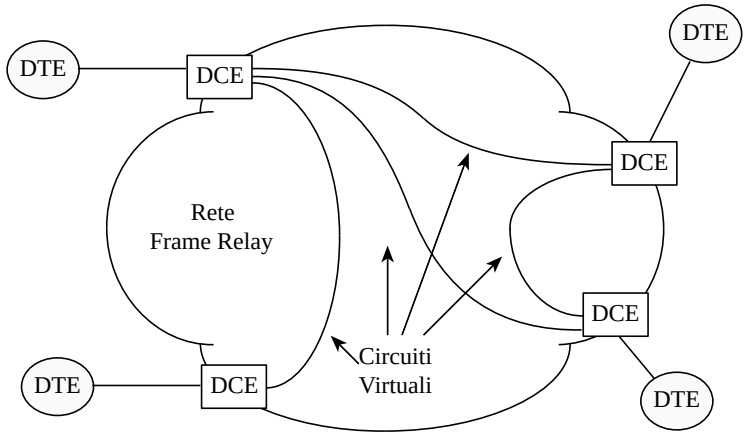


Fig. 13.11 - Rete Frame Relay.

I circuiti virtuali sono permanenti, cioè creati dal gestore della rete, anche se esistono proposte per avere in futuro la possibilità di creare circuiti virtuali temporanei.

13.5.2 L'evoluzione di Frame Relay

Frame Relay è il risultato ottenuto nel 1990 da un consorzio di ditte appositamente creato, di cui facevano parte Cisco, Digital Equipment, Northern Telecom e Stratacom.

Il consorzio si è basato sugli standard proposti in sede CCITT nell'ambito del progetto ISDN ed in particolare sulle raccomandazioni I.122 e Q.922.

Il consorzio ha però proposto numerose e significative estensioni agli standard CCITT, globalmente dette LMI *(Local Management Interface).*

13.5.3 Il livello Data Link di Frame Relay

Lo standard Q.922, che specifica il *data link layer protocol and frame mode bearer services*, si basa sullo standard CCITT Q.921 LAPD (*Link Access Procedure on the D-channel*) e lo estende, formando il LAPF (*Link Access Procedure to Frame mode bearer services*).

Il LAPD e il LAPF utilizzano il flag, come in HDLC, per marcare l'inizio e la fine delle trame, e adottano l'algoritmo di bit stuffing (si veda il paragrafo 13.2.5), per garantire la trasparenza della trasmissione.

Il protocollo LAPF è suddiviso in due parti:

- DL-CORE (*Data Link Core protocol*) definito nella raccomandazione CCITT I.233;
- DL-CONTROL (*Data Link Control protocol*), la rimanente parte di LAPF.

Il formato del pacchetto Frame Relay è mostrato in figura 13.12, dove in grigio sono stati evidenziati i campi ignorati dalle funzionalità di DL-CORE.

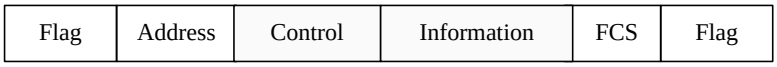


Fig. 13.12 - Pacchetto Frame Relay.

Il significato dei campi di DL-CORE è il seguente:

- Flag, come in HDLC;
- Address, un indirizzo esteso con funzionalità di controllo delle congestioni con lunghezza pari a 2, 3 o 4 ottetti (figura 13.13);
- FCS, una CRC su 2 ottetti.

In particolare, il campo address è suddiviso in una serie di sottocampi (figura 13.13) il cui significato è il seguente:

- EA (*Address field extension bit*), se a uno, indica l'ultimo ottetto del campo address;

- C/R (*Command/Response*), riservato per usi futuri;
- FECN (*Forward Explicit Congestion Notification*), bit posto a uno dalla rete Frame Relay per segnalare ai router che il cammino percorso dalla trama presenta delle tratte congestionate;
- BECN (*Backward Explicit Congestion Notification*), bit posto a uno dalla rete Frame Relay per segnalare ai router che il cammino in direzione opposta a quello percorso dalla trama presenta delle tratte congestionate;
- DLCI (*Data Link Connection Identifier*), è l'identificatore del circuito logico ed è il sottocampo principale del campo address; lungo normalmente 10 bit ha un significato locale alla connessione DTE-DCE e quindi connessioni diverse, su nodi diversi, possono avere lo stesso DLCI;
- DE (*Discard Eligibility indicator*), se a uno, indica che la trama può essere scartata in presenza di congestione della rete;
- D/C (*DLCI or DL-CORE control indicator*), indica se i rimanenti 6 bit dell'ottetto debbano essere interpretati come DLCI o come DL-CORE control.

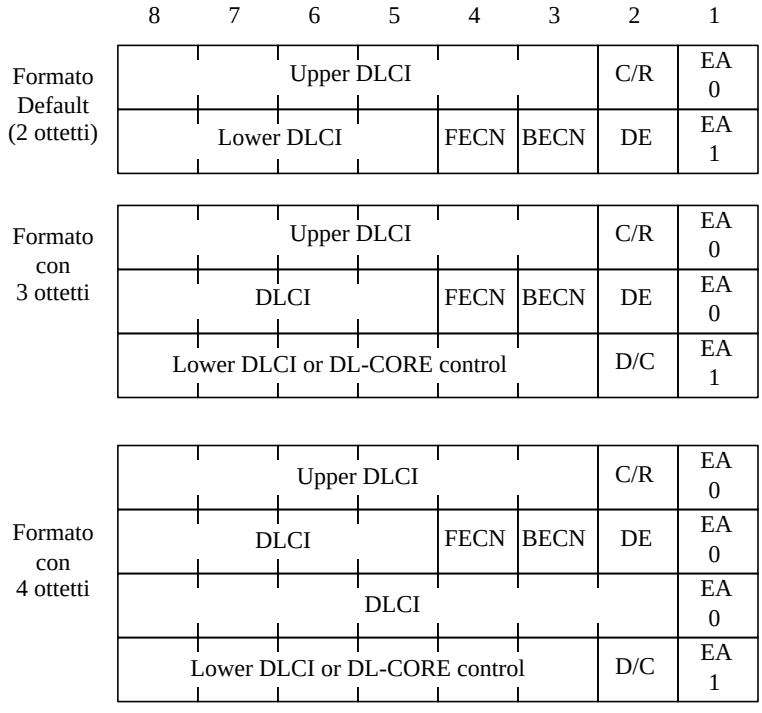


Fig. 13.13 - Il campo Address

Una rete Frame Relay può essere realizzata da un insieme di commutatori Frame Relay (nodi *core*) che instradano il messaggio sulla base del DLCI, realizzando solo la parte di LAPF detta DL-CORE, mentre i nodi terminali (nodi *edge*) realizzano sia il DL-CORE, sia il DL-CONTROL (figura 13.14).

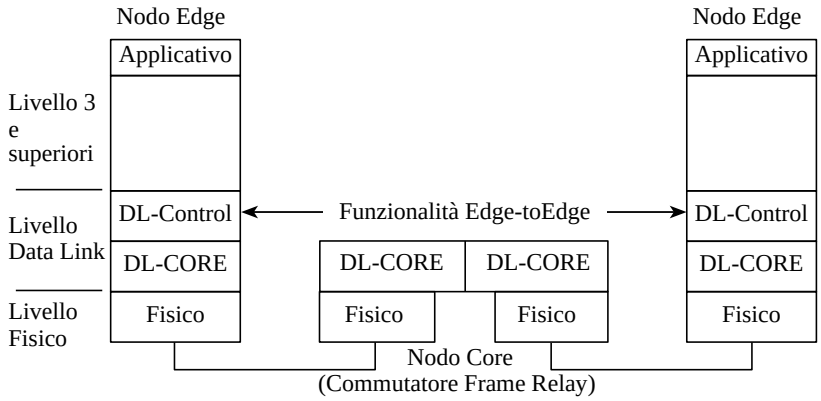


Fig. 13.14 - Esempio di rete Frame Relay.

Tale approccio è detto *core-edge*, in quanto alcune funzionalità vengono realizzate solo edge-to-edge (ad esempio, recupero di errori o controllo di flusso).

La struttura del campo control di figura 13.12 è specificata nella raccomandazione Q.922 e ricalca quella del campo control di HDLC (figura 13.2). La numerazione delle trame, se presente, viene effettuata modulo 128 (su 7 bit), quindi il campo control ha dimensioni pari a un ottetto per gli U-frame e a 2 ottetti per gli S-frame e gli I-frame.

13.5.4 Le trame LMI

Le trame LMI sono state concepite per contenere le estensioni proposte dal consorzio Frame Relay, ma tali estensioni sono state riprese da ANSI e CCITT che le hanno modificate e rese standard. Le versioni standard sono oggi più diffuse di quelle originali.

La figura 13.15 mostra il formato di una trama LMI.

Ottetti

1	2	1	1	1	1	variabile	2	1
Flag	LMI DLCI	UI	Protocol discriminator	Call reference	Message type	IE	FCS	Flag

Fig. 13.15 - Formato di una trama LMI.

Le trame LMI sono identificabili a livello DL-CORE poiché inviate sul DLCI 1023. A livello DL-Control sono trame di tipo Unnumbered Information (UI).

Il campo *protocol discriminator* contiene un valore fisso che indica il protocollo LMI.

Il campo *call reference* contiene sempre il valore zero.

Il campo *message type* indica i due tipi di messaggi ammessi: status-enquiry e keepalives.

Il campo *Information Elements (IE)* contiene un primo ottetto detto *IE identifier*, un secondo ottetto di *IE length* e altri ottetti contenenti le informazioni di management del protocollo LMI.

I messaggi di *status-enquiry* permettono ad un nodo di chiedere ed ottenere informazioni sullo stato della rete. Tali messaggi verificano l'integrità dei collegamenti fisici e logici e permettono agli algoritmi di routing di prendere le opportune decisioni in funzione dello stato della rete.

I messaggi di *keepalives* vengono inviati periodicamente da ogni nodo per informare l'altra estremità della connessione che la connessione continua ad essere attiva.

Oltre alle prestazioni classiche di LMI esistono due estensioni importanti: *global addressing* e *multicasting*.

13.5.5 Global Addressing

I nodi Frame Relay non hanno un indirizzo: ad avere indirizzo sono i canali logici (DLCI). Questo è un limite quando si vogliono realizzare reti di grosse dimensioni, poiché impone l'uso di tabelle statiche sui router e inibisce l'utilizzo di protocolli quali ARP/RARP (si veda paragrafo 16.7).

Il global addressing è una estensione che assegna ad ogni nodo Frame Relay un DLCI univoco che diventa il suo indirizzo sulla rete. Questo permette di migliorare l'utilizzo di una rete Frame Relay da parte dei router che, con il global addressing, la vedono equivalente ad una LAN.

13.5.6 Multicasting

I protocolli per il calcolo automatico delle tabelle di instradamento dei router (si veda il paragrafo 14.5.3) necessitano spesso di inviare un messaggio in multicast a tutti i router presenti sulla rete.

L'estensione multicasting di Frame Relay serve a soddisfare tale esigenza.

Vengono riservati quattro valori di DLCI (da 1019 a 1022). L'estensione LMI invia notifiche ai nodi riguardo alla creazione, presenza e cancellazione dei gruppi di multicast.

Un messaggio inviato ad un DLCI associato ad un gruppo di multicast è replicato e trasmesso a tutti i nodi appartenenti al gruppo.

13.6 SMDS

SMDS (Switched Multi-megabit Data Service) è stato proposto da Bellcore (Bell Communication Research) nel 1987 per offrire un servizio pubblico, non connesso, ad alte prestazioni con lo standard TR-772 (Technical Requirements 772). SMDS è particolarmente adatto a realizzare internetworking di LAN.

SMDS fornisce velocità comprese nell'intervallo tra 2 e 34 Mb/s e le BOC (Bell Operanting Company) offrono servizi SMDS nell'America del Nord già dal 1990.

In Europa SMDS viene detto anche CBDS *(Connectionless Broadband Data Service)* ed esiste un gruppo di interesse europeo denominato ESIG *(European SMDS Interest Group).*

Ancora una volta SMDS è uno standard che specifica solo l'interfaccia DTE-DCE e non come è organizzata la rete al suo interno. Il protocollo di interfaccia è detto SIP *(SMDS Interface Protocol)* e il punto di demarcazione tra la rete SMDS e gli apparati di utente è detto SNI *(Subscriber Network Interface).*

La figura 13.16 mostra un esempio di utilizzo di SMDS per interconnettere due LAN Ethernet tramite router.

SIP si basa sullo standard per le reti metropolitane DQDB (*Distributed Queue Dual Bus*) descritto nel capitolo 9. Il protocollo SIP ha due tipi di PDU, dette L3PDU* e L2PDU.

Il router genera le L3PDU e le invia all'unità CSU/DSU (*Channel Service Unit / Data Service Unit*) che le frammenta in L2PDU e le trasmette sulla rete. L'unità CSU/DSU all'altro estremo della rete effettua il procedimento inverso.

Il router e la CSU/DSU, per scambiarsi le L3PDU, le incapsulano in una trama HDLC. Il formato di incapsulamento più diffuso è detto DXI (*Data eXchange Interface*).

Le L3PDU hanno una forte analogia con le IMPDU del DQDB (figura 9.12), mentre le L2PDU hanno una forte analogia con gli slot DQDB (figura 9.8) che a loro volta contengono le DMPDU (figura 9.14).

* Attenzione: L3 in questo caso non significa livello 3 OSI, in quanto sia le L3PDU, sia le L2PDU, appartengono al livello 2 OSI.

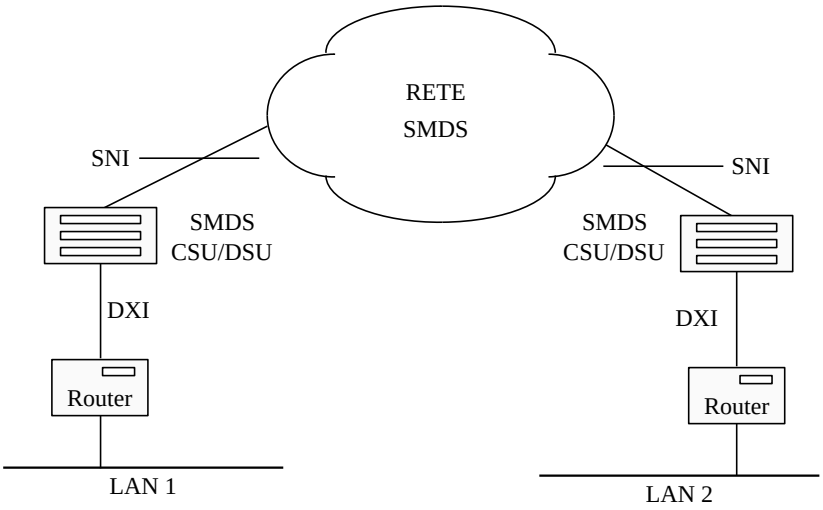


Fig. 13.16 - Esempio di utilizzo di SMDS.

La relazione tra le L3PDU e le L2PDU è mostrata in figura 13.17.

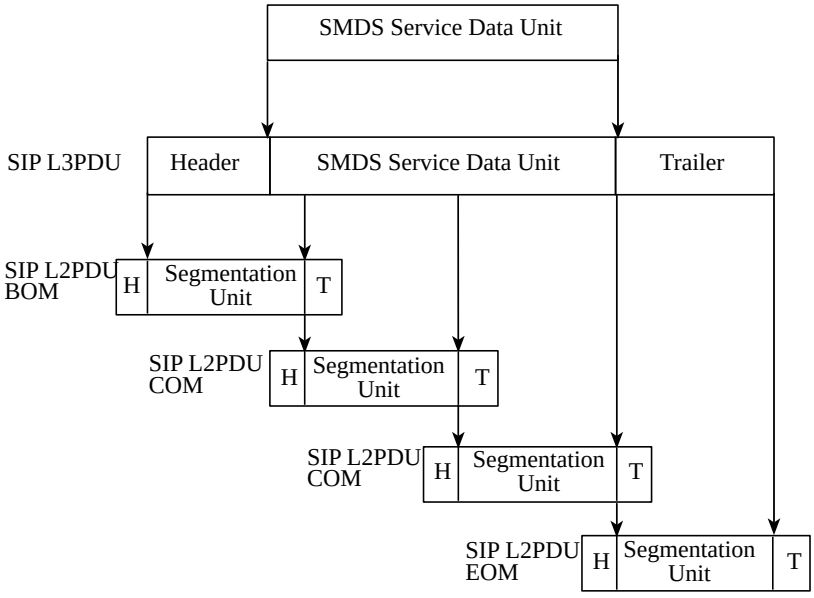


Fig. 13.17 - SMDS Protocol Data Unit.

SMDS non si occupa di fornire un supporto standard per la convivenza di più protocolli. Per questa ragione la SMDS SDU può contenere una LLC-PDU che con i classici meccanismi delle reti locali (si veda il paragrafo 5.7.3) fornisce il supporto multiprotocollo. In particolare lo RFC 1209 indica come usare le SNAP PDU per trasportare i pacchetti IP (si veda il paragrafo 5.7.4).

La figura 13.18 mostra un esempio di internetworking in ambito OSI (si veda paragrafo 17.5) utilizzando SMDS.

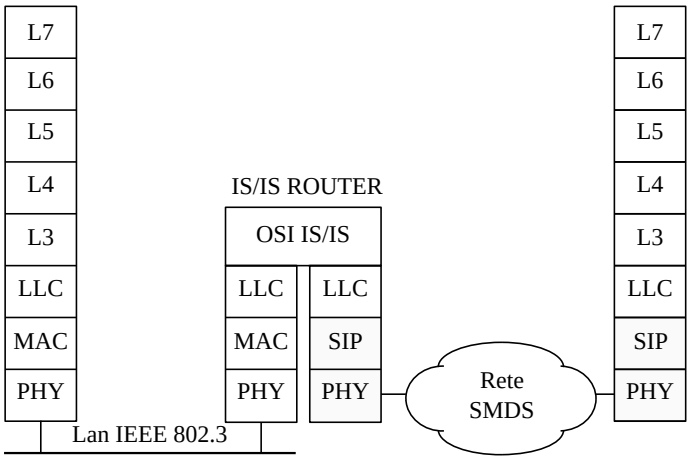


Fig. 13.18 - Internetworking OSI tramite SMDS.

L'indirizzamento SMDS è basato sullo standard E.164 e presenta interessanti funzionalità aggiuntive quali:

- più indirizzi per una singola interfaccia;
- indirizzi di gruppo, cioè un indirizzo identifica un insieme di interfacce: questo è molto utile per la gestione del traffico di broadcast;
- validazione del Source Address dichiarato dall'apparato di utente da parte della rete: questa funzionalità è molto importante per la sicurezza, perché previene i tentativi di connessioni illecite (*address spoofing*).

SMDS fornisce inoltre un sofisticato meccanismo di negoziazione del throughput, tramite la definizione di una *access class* e di un grado di *burstiness* (varianza del *throughput*). Sulle interfacce a velocità superiori tale meccanismo è realizzato da un *credit manager.*

13.7 ANALISI COMPARATA

La tabella 13.2 mostra un'analisi comparata delle tecnologie a commutazione di pacchetto descritte in questo capitolo. Per completezza è inclusa anche la tecnologia ATM, che verrà descritta nei capitoli 19, 20 e 21.

Prestazione	X.25	Frame Relay	SMDS	ATM
Standard	CCITT, ISO, ...	CCITT, ANSI	Bellcore, ETSI	CCITT
Velocità tipica	9.6 - 64 kb/s	64kb/s - 2Mb/s	2 - 34 Mb/s	45 - 155 Mb/s
Dimensione del pacchetto	Variabile sino a 4096 byte	Variabile sino a 4096 byte	Variabile sino a 9188 byte	Fissa 53 byte
Multicasting	No	Si, scarsamente realizzato	Sì	Proposta
Indirizzi	X.121 a lunghezza variabile, sino a 14 cifre	DLCI a lunghezza fissa, normalmente 10 bit	Lunghezza variabile sino a 15 cifre per formato E.164	VPI/VCI lunghezza fissa 24 bit
Connectionless	No	No	Sì	No
PVC	Sì	Sì	N.A.	Sì
SVC	Sì	Proposta	N.A.	Sì
Controllo di flusso per circuito virtuale	Sì	No	N.A.	No
Correzione degli errori su ogni tratta	Sì	No	No	No

N.A.: Non Applicabile

Tab. 13.2 - Tecnologie a commutazione di pacchetto.

BIBLIOGRAFIA

[1] ISO 3309, "HDLC Procedures - Frame Structure", 1979.

[2] ISO 3309/PDAD1, "Addendum 1: Start/Stop transmission", 1984.

[3] ISO 4335, "HDLC Elements of Procedures", 1979.

[4] ISO 7776, "HDLC Procedures - X.25 LAPB-compatible DTE Data Link Procedures".

[5] ISO 7809, "HDLC Procedures - Consolidation of Classes of Procedures"

[6] ISO 8471, "HDLC Data Link Address Resolution".

[7] ISO 8885, "HDLC Procedures - General purpose XID Frame Information Field Contents and Format".

[8] W. Simpson, "RFC 1548: The Point-to-Point Protocol (PPP)", September 1993.

[9] X.3 "Packet assembly/disassembly facility (PAD) in a Public Data Network".

[10] X.25 "Interface between DTE and DCE for Terminal Operating in the Packet Mode and Connected to Public Data Network by Dedicated Circuit".

[11] X.28 "DTE/DCE Interface for Start-Stop Mode DTE Accessing the PAD Facility in a Public Data Network Situated in the Same Country".

[12] X.29 "Procedures for the Exchange of Control Information and User Data between a PAD facility and a Packet Mode DTE or another PAD".

[13] X.32 "Interface between DTE and DCE for Terminal Operating in the Packet Mode and Accessing a Packet Switched Public Data Network through a Public Switched Telephone Network or a Circuit switched Public Data Network".

[14] X.75 "Terminal and Transit Call Control Procedures and Data Transfer System on International Circuits between Packet-Switched Data Network".

[15] X.121 "International Number Planning for Public Data Network".

[16] I.122, "Framework for Frame Mode Bearer Services", ITU-T, March 1993

[17] I.233, "Frame Mode Bearer Services", CCITT, Geneva.

[18] Q.921, "ISDN user-network interface-Data link layer specification", CCITT, Geneva.

[19] Q.922, "ISDN Data Link Layer Specification for Frame Mode Bearer Services", CCITT, Geneva, 1992.

[20] T. Bradley, C. Brown, A. Malis, "RFC 1294: Multiprotocol Interconnect over Frame Relay", January 1992.

[21] "Generic System Requirements in Support of Switched Multi-Megabit Data Service"Bellcore, TR-TSV-000772, Issue 1, May 1991.

[22] D. Piscitello, J. Lawrence, "RFC 1209: The transmission of IP Datagrams over the SMDS Service", March 1991.

14

LE TECNICHE DI INTERNETWORKING

14.1 INTRODUZIONE

Nel capitolo 2 è stato introdotto il modello di riferimento OSI. In tale modello una rete di calcolatori viene vista come un insieme di sistemi interconnessi tra loro. Su alcuni sistemi (gli ES: *End System*) risiedono le applicazioni che comunicano usando la rete, altri sistemi hanno funzioni di instradamento dei messaggi (gli IS: *Intermediate System*).

Un primo problema consiste nella necessità di identificare in modo univoco ciascun sistema sulla rete. A tal scopo, ad ogni sistema è associato un *indirizzo* numerico (una serie di byte).

Tuttavia, nella maggior parte dei casi, è molto più comodo per l'utente riferirsi ad un sistema utilizzando un *nome* piuttosto che un indirizzo numerico. Il nome e l'indirizzo di un sistema hanno la stessa finalità, cioè quella di identificare in modo univoco un sistema all'interno della rete.

Occorre chiaramente mantenere una relazione biunivoca tra gli indirizzi e i nomi, e questo è più complesso di quanto si possa pensare. Infatti in una rete piccola è pensabile che ogni singolo calcolatore abbia un file che mantiene tale corrispondenza, ma al crescere delle dimensione della rete è indispensabile dotarsi di una base dati distribuita, detta *name server*.

In modo analogo occorre mantenere delle tabelle di corrispondenza tra i nomi degli applicativi e i loro indirizzi (spesso detti anche identificatori di *porta*) che li identificano in modo univoco all'interno del sistema.

Quando un utente desidera connettersi ad un applicativo su di un dato elaboratore, egli lo richiede alla rete che, consultando la base dati, ricava l'identificativo della porta e l'indirizzo dell'elaboratore.

L'indirizzo dell'elaboratore destinatario del messaggio diventa l'elemento chiave con cui si determina l'instradamento più idoneo a raggiungere il sistema remoto. Un

primo controllo che il mittente effettua è quello di verificare se il destinatario è sulla stessa "rete": in questo caso la trasmissione può avvenire direttamente.

In caso contrario, è indispensabile un'operazione di *internetworking*: il mittente affida il pacchetto ad un IS che si occuperà di farlo giungere a destinazione.

14.1.1 Tecniche di instradamento

Quando un IS riceve un pacchetto deve effettuare un'operazione di instradamento, cioè ritrasmettere il pacchetto verso il destinatario finale. La tecnica di instradamento scelta dipende dall'architettura di rete adottata. Esistono tre tecniche principali:

- *Routing by network address*. Un sistema è indirizzato scrivendo nel pacchetto il suo indirizzo, che deve essere univoco sulla rete. Ogni IS usa tale indirizzo come chiave di ricerca nella sua tabella di instradamento e determina lungo quale cammino il pacchetto debba essere ritrasmesso. Tale tecnica è usata nei transparent-bridge, in DECnet, in OSI-CLNS e in IP. È in generale adottata dai protocolli non connessi.
- *Label swapping*. È generalmente usata nei protocolli connessi e trova applicazioni in ATM (si veda il paragrafo 19.2) e in APPN (si veda il paragrafo 18.3). Ogni pacchetto è marcato con una label che serve come chiave in una tabella di instradamento sull'IS. L'IS, prima di ritrasmettere il pacchetto, sostituisce la label con una nuova label. Le label devono quindi essere univoche solo all'interno di un dato link. Se il protocollo è connesso, le label altro non sono che gli identificativi delle connessioni.
- *Source routing*. È una tecnica usata, ad esempio, dai bridge Token Ring (si veda il paragrafo 10.18). Nel source routing l'instradamento completo, cioè la lista degli IS da attraversare, è scritto nel pacchetto dal nodo mittente, che lo chiede ad un IS o lo scopre con meccanismi di "route location". Il source routing è utilizzato in APPN+.

Quanto sin qui descritto prescinde dal livello a cui viene effettuato l'instradamento. L'OSI delega la funzionalità di instradamento al livello 3 Network (o rete) e in particolare agli IS, spesso detti router. Altre architetture preferiscono affettuare l'instradamento a livello 2, utilizzando dei bridge.

Esempi di reti che instradano a livello 3 sono OSI, X.25, DECnet e IP. Esempi di reti con istradamento a livello 2 sono le BLAN (LAN estese con bridge), Frame Relay, e SMDS. Esistono poi reti in cui la distinzione tra i due livelli non è più così netta, ad esempio in HPR/APPN+.

Se si considerano i bridge source routing, è difficile motivare perché essi siano

considerati dei bridge e non dei router, visto che operano nella terza modalità precedentemente elencata. Sono stati definiti bridge principalmente perché il comitato di standardizzazione che se ne è occupato apparteneva al progetto IEEE 802 che tratta esclusivamente i livelli Fisico e Data Link.

Lungi dal voler entrare in questa diatriba, nel seguito del libro si farà riferimento al modello OSI classico e si assumerà, quando non diversamente specificato, che l'internetworking avvenga a livello 3 in modalità routing by network address.

14.1.2 Indirizzi

Su reti ad accesso multiplo come le LAN si devono anche di stabilire delle relazioni tra gli indirizzi di livello 2 sottolivello MAC e gli indirizzi di livello 3 (Network) per poter effettuare l'instradamento. Lo scopo dei due tipi di indirizzo è diverso:

- l'indirizzo di livello 2 MAC, come già visto nel paragrafo 5.6.7, serve a discriminare il destinatario finale di un pacchetto nell'ambito di una LAN;
- l'indirizzo di livello 3 serve invece ad identificare il destinatario finale del pacchetto nell'ambito dell'intera rete.

È ragionevole ipotizzare che un nodo abbia tanti indirizzi di livello 2 MAC quante sono le sue schede di rete locale ed un solo indirizzo di livello 3. Questo è vero nella maggior parte dei protocolli con un'unica eccezione di rilievo: il TCP/IP. Infatti il protocollo IP ha un indirizzo di livello 3 per ogni scheda di rete LAN o WAN (si veda paragrafo 16.5).

Nell'ambito di una LAN esistono vari metodi per mantenere le corrispondenze tra gli indirizzi di livello 2 MAC e gli indirizzi di livello 3: il più diffuso si basa sull'utilizzo del protocollo ARP (*Address Resolution Protocol*) descritto nel paragrafo 16.7.

Vediamo tramite l'esempio riportato in figura 14.1 il ruolo dei due tipi di indirizzi.

Si supponga di dover trasmettere un pacchetto dall'ES B all'ES A. La trasmissione avviene nelle seguenti quattro fasi, mediante tre pacchetti diversi identificati con (a), (b), e (c) in figura 14.1:

- B genera un pacchetto di livello 3 con L3-DSAP=A e L3-SSAP=B che rimarrà immutato sino a destinazione. B verifica se A è sulla sua stessa LAN e poiché ciò non è vero invia il messaggio a R2 specificando L2-DSAP=R2 e L2-SSAP=B (pacchetto (a)).
- L'IS R2 riceve il pacchetto (a) ed utilizza le sue tabelle di instradamento per decidere di ritrasmettere il messaggio sul Canale Diretto Numerico (CDN). In questo caso, poiché ci troviamo in presenza di un canale punto-punto, non è necessaria la presenza di un indirizzo a livello 2 nel pacchetto (b).

- R1 riceve il pacchetto (b) e decide che deve trasmetterlo ad A tramite la LAN. Usando, ad esempio, un algoritmo di ARP ricava l'indirizzo di livello 2 di A a partire dal suo indirizzo di livello 3 e quindi effettua la trasmissione del pacchetto (c).
- A riceve il pacchetto (c) e, poiché lo L3-DSAP è uguale al suo indirizzo di livello 3, non lo inoltra ulteriormente sulla rete, ma lo passa ai suoi livelli superiori.

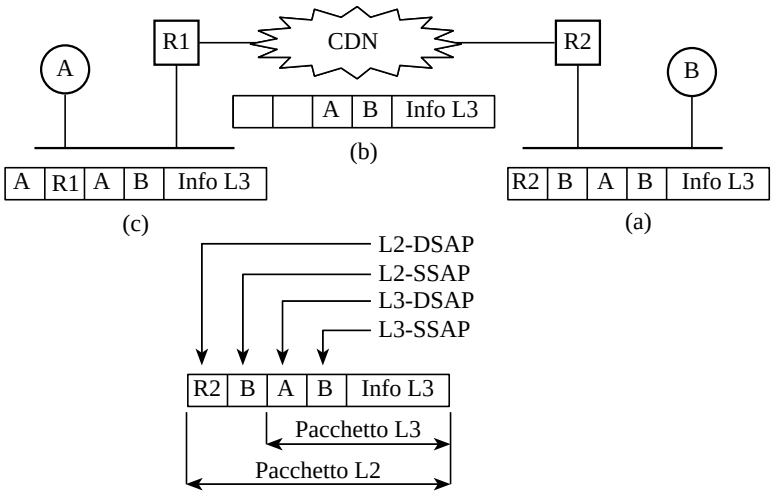


Fig. 14.1 - Indirizzi MAC e Network.

14.1.3 L'instradamento

Esaminiamo più nel dettaglio la funzionalità di instradamento dei router, cioè degli Intermediate System operanti a Livello 3, con l'ausilio della figura 14.2.

Un pacchetto viene ricevuto dal router tramite una sua scheda di LAN o di WAN che gestisce un protocollo di livello 2. La scheda verifica se il pacchetto è destinato al router (condizione sempre vera su linee punto-punto, ma da verificarsi tramite gli indirizzi MAC sulle LAN) e in caso affermativo lo passa al processo di forwarding. Questo determina su quale linea deve essere ritrasmesso il pacchetto consultando le tabelle di instradamento.

Le tabelle di instradamento possono essere scritte manualmente dal gestore della rete oppure calcolate automaticamente da un opportuno algoritmo. Tale algoritmo opera scambiando tra gli IS informazioni relative alla topologia e allo stato della rete.

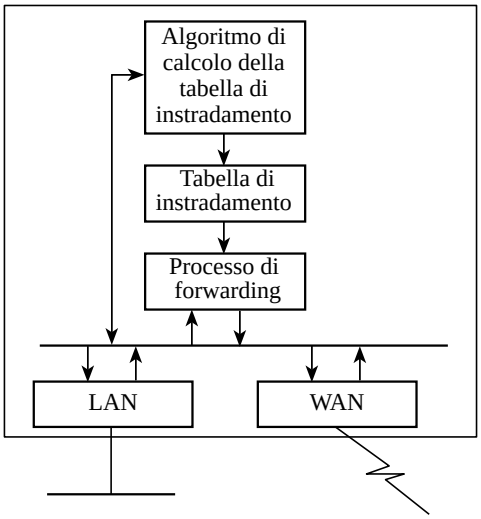


Fig. 14.2 - Architettura di un router.

14.1.4 Neighbor Greetings

Un altro problema è quello dei "neighbor greetings", cioè del fatto che gli IS collegati ad una LAN devono conoscere gli ES collegati alla stessa LAN e viceversa. Questo è indispensabile per due motivi:

- gli IS devono conoscere gli ES per inserirli nelle tabelle di instradamento e propagare l'informazione della loro raggiungibilità agli altri IS;
- gli ES devono conoscere gli IS presenti sulla LAN per sapere a chi inviare i messaggi non destinati a nodi collegati alla stessa LAN.

La soluzione a quest'ultimo problema deve essere tale da ammettere LAN prive di router, LAN con un solo router o LAN con più router.

14.1.5 L'internetworking multiprotocollo

A differenza dei bridge che sono assolutamente trasparenti al protocollo di livello 3, nel senso che ignorano il contenuto del campo Info di livello 2, i router operano a livello 3 e quindi utilizzano per l'internetworking tutte le informazioni contenute nella busta di livello 3.

Le buste di livello 3 delle diverse architetture di rete (es. TCP/IP, DECnet, OSI)

hanno formati e contenuti tra loro incompatibili, quindi i router sono progettati facendo riferimento ad un dato formato del pacchetto di livello 3 e quindi ad una data architettura di rete.

Chiaramente, disporre oggi di router in grado di trattare una sola architettura di rete sarebbe inaccettabile e da alcuni anni sono disponibili sul mercato router multiprotocollo che hanno una struttura più complessa, riportata in figura 14.3.

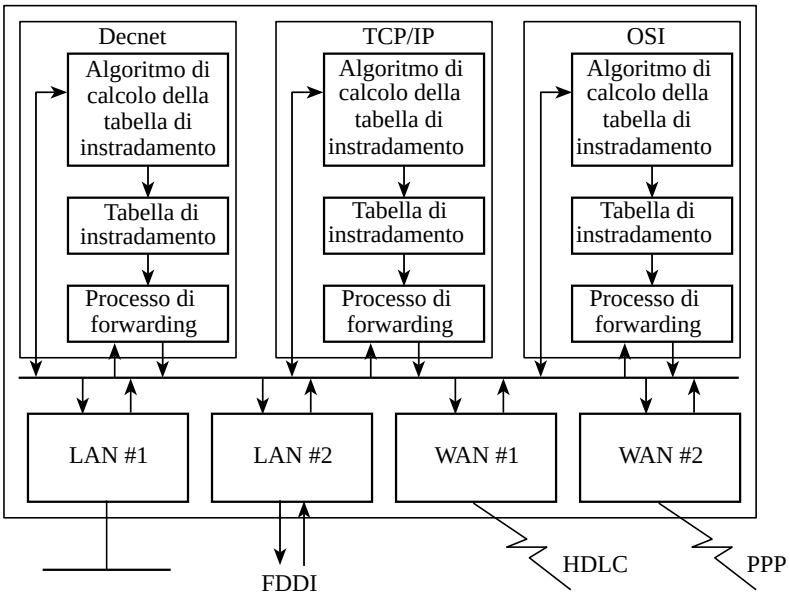


Fig. 14.3 - Router multiprotocollo.

Da una prima analisi si vede che il modulo di instradamento è replicato per ogni protocollo trattato. Molto spesso esiste anche un modulo di bridging per trattare quei protocolli che non hanno un livello 3 (es: LAT, NetBeui, MOP) e che quindi non sarebbero gestibili dai router. Quando un router multiprotocollo realizza anche la funzionalità di bridging viene detto *brouter*.

Un brouter è in grado, protocollo per protocollo, di:

- non trattare il protocollo e quindi scartare eventuali pacchetti appartenenti a quel protocollo;
- trattare il protocollo tramite una modalità di bridging, quindi a livello 2;
- trattare il protocollo tramite una modalità di routing, quindi a livello 3.

L'ultima opzione è possibile solo se l'architettura di rete ha un livello 3 e quindi è instradabile. Come già accennato precedentemente, esistono architetture di rete

quali il LAT (si veda l'appendice B, paragrafo B.5) , il Netbeui, il MOP e altre che, essendo state progettate pensando ad un utilizzo esclusivamente su rete locale, non hanno un livello 3. Se si vuole poter utilizzare tali architetture anche su base geografica l'unica possibilità è l'impiego della funzionalità di bridging.

Possiamo ora precisare meglio il ruolo degli indirizzi di livello 2. Nell'esempio precedente gli indirizzi di livello 2 citati sono indirizzi di livello 2 MAC, poiché servono a gestire la trasmissione sulla LAN. Gli indirizzi di livello 2 LLC non hanno come scopo l'indirizzamento di un nodo, ma di una architettura di rete all'interno di un nodo.

Supponiamo che un pacchetto venga ricevuto dal router multiprotocollo di figura 14.3 sulla scheda LAN#1. La scheda tramite l'indirizzo L2-MAC determina se il pacchetto è destinato al router e quindi, tramite l'indirizzo L2-LLC, determina a quale modulo di instradamento passare il pacchetto (nell'esempio, DECnet, TCP/IP o OSI). Il modulo di instradamento, ricevuto il pacchetto, determina tramite l'indirizzo di livello 3 su quale linea e a quale nodo ritrasmettere il pacchetto.

A questo punto il lettore dovrebbe essersi fatto un'idea dei molti problemi da affrontare per instradare un messaggio su una rete. Altri problemi sono la gestione di topologie complesse, la convivenza di più mezzi trasmissivi diversi, l'organizzazione gerarchica della rete, ecc.

I paragrafi seguenti analizzano questi problemi in modo più approfondito.

14.2 IL LIVELLO NETWORK

Una rete di calcolatori si realizza interconnettendo con vari tipi di tecnologie (linee telefoniche commutate, CDN, X.25, ISDN, SMDS, Frame Relay, LAN, ATM) un insieme di IS (commutatori di pacchetto) normalmente chiamati *router* (figura14.4).

Gli IS si occupano di instradare i messaggi sulla rete ed operano al livello 3 del modello di riferimento OSI, cioè a *livello Network*.

Alcuni router sono a volte detti anche IMP (*Interface Message Processor*) o IP Gateway*.

Il termine *nodo* viene spesso adottato in luogo del più corretto termine *sistema*. Un nodo è un dispositivo di rete che contiene al suo interno almeno i livelli Fisico, Data Link e Network.

* Il termine IP Gateway di derivazione TCP/IP è particolarmente infelice in quanto OSI assegna un altro significato al termine gateway e per questo motivo se ne sconsiglia l'uso e in questo libro non verrà adottato.

Gli ES (detti anche end node) sono quei nodi che agiscono come mittente e destinatario finale dei dati e tipicamente implementano tutti e sette i livelli del modello di riferimento OSI. Essi hanno un livello 3 molto semplice in quanto non devono preoccuparsi delle problematiche di instradamento.

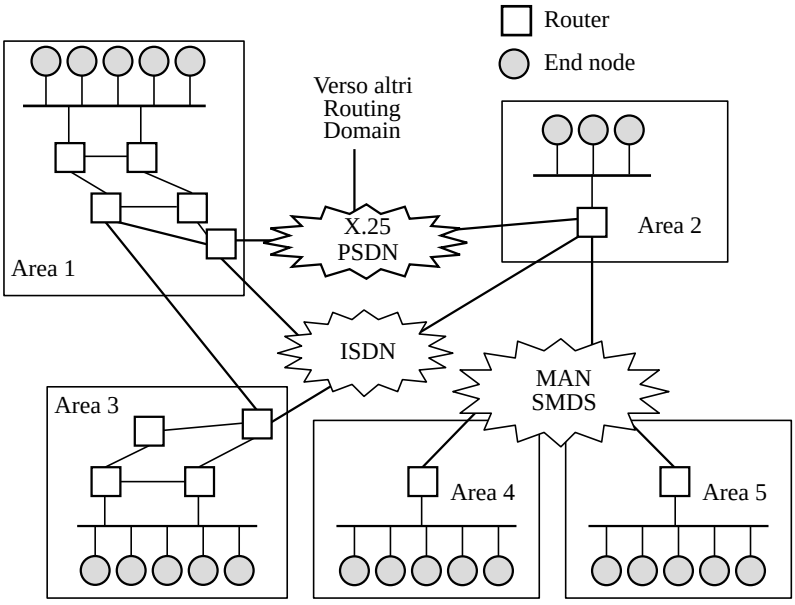


Fig. 14.4 - Esempio di WAN con router.

Molto spesso a livello 3, oltre al protocollo per trasportare i dati di utente, sono definiti anche uno o più protocolli ausiliari per il neighbor greetings e per permettere ai router di scambiarsi informazioni di instradamento.

La necessità di realizzare funzionalità di gestione (management) del router rende necessaria la presenza negli IS anche di protocolli specifici per la gestione*, che sono collocati nei livelli superiori al terzo.

Per instradare i pacchetti, il livello network si basa sull'indirizzo del destinatario finale e sulle tabelle d'instradamento presenti negli IS. Le tabelle d'instradamento possono essere scritte manualmente (soluzione adottata nella rete SNA e a volte anche

* Il protocollo di gestione, che è ormai oggi uno standard "de facto" e con cui si opera normalmente sui router e sulla altre apparecchiature di rete, è il SNMP (*Simple Network Management Protocol*), che si basa su UDP/IP (si veda il paragrafo 16.12.9).

in quella TCP/IP) o calcolate automaticamente mediante algoritmi che apprendono la topologia della rete e si adattano ai suoi cambiamenti, determinando instradamenti alternativi in caso di guasti.

Il livello Network può offrire servizi di tipo connesso (*connection oriented*) e non connesso (*connectionless*). L'implementazione dei servizi connessi (CONS) a questo livello avviene tramite i circuiti virtuali. Il CCITT e le PTT sono forti sostenitori di questa filosofia, che è realizzata in reti dati a pacchetto, quali quelle conformi ai protocolli X.25 e Frame Relay.

I servizi non connessi (CLNS) a questo livello prendono anche il nome di servizi di *datagram*; essi sono adottati nelle reti proprietarie quali DECnet e TCP/IP, proposti dall'ISO per le reti OSI nello standard ISO 8473 e realizzatti da alcune PTT in reti come quelle conformi allo standard SMDS (si veda paragrafo 13.6).

La tabella 14.1 riassume alcune proprietà dei servizi connection oriented e connectionless, rispetto ad una serie di caratteristiche, che possiamo considerare ai fini di un confronto.

Caratteristica	Connection Oriented	Connectionless
Setup Iniziale	Richiesto	Impossibile
Destination Address	Durante il setup	Ad ogni pacchetto
Ordine dei Pacchetti	Garantito	Non garantito
Controllo Errori	A livello Network	A livello trasporto
Controllo di Flusso	Fornito dal Network	Non fornito dal Network
Negoziazione delle Opzioni	Sì	No
Uso di Connection Identifier	Sì	No

Tab. 14.1 - Confronto tra L3 connesso e non connesso.

Per quanto riguarda il controllo dell'errore, bisogna ricordare che, anche se esso viene implementato al livello 3, solitamente l'affidabilità non è considerata sufficiente ai livelli superiori e quindi il livello 4 è comunque connesso.

14.3 ALGORITMI DI INSTRADAMENTO

La scelta di un algoritmo di instradamento è difficile, in quanto esistono più criteri di ottimalità spesso contrastanti, ad esempio minimizzare il ritardo medio di ogni

pacchetto o massimizzare l'utilizzo delle linee.

Occorre che la scelta sia preceduta dalla definizione di criteri misurabili. Occorre cioè introdurre dei parametri metrologici in base ai quali misurare le caratteristiche di un cammino per scegliere, ad esempio, il migliore tra due cammini alternativi.

Gli unici due parametri universalmente accettati sono:

- il numero di salti effettuati (*hop*), cioè il numero di IS attraversati lungo un cammino;
- il *costo*, cioè la somma dei costi di tutte le linee attraversate lungo un cammino.

Entrambi questi parametri sono di demerito, in quanto il costo di una linea è assegnato in modo inversamente proporzionale alla velocità della linea stessa, e gli hop indicano router attraversati e quindi ritardi introdotti.

Metriche che tengano in considerazione il carico della rete sono più difficili da mettere a punto, in quanto portano facilmente a situazioni di routing instabile. Le tecniche più moderne consentono al più di operare un *load splitting* (bilanciamento del traffico) tra cammini paralleli, eventualmente attivando circuiti commutati, quali quelli forniti dalla rete ISDN (si veda paragrafo 12.6) in presenza di un guasto (ad esempio, funzionalità di backup di un CDN) o per gestire un eccesso di traffico su di un link (traffico di trabocco).

La scelta dell'algoritmo di instradamento ottimale è anche complicata dalle limitate risorse di memoria e CPU disponibili oggi sui router, specialmente se confrontate con la complessità delle reti ed in particolare con l'elevato numero di nodi collegabili con una topologia qualsiasi. Algoritmi troppo complessi, operanti su reti molto grandi, potrebbero richiedere tempi di calcolo inaccettabili.

I router attualmente installati sulle reti vanno dai vecchi router con CPU da 1 MIPS e con memoria da 1 Mbyte, ai più moderni router con più CPU RISC da 25 MIPS e memoria da 16 Mbyte. Uno dei fattori che limita la produzione di router sempre più potenti è soprattutto il costo, che deve mantenersi ragionevolmente contenuto.

Riassumendo, le caratteristiche che in generale si richiedono ad un algoritmo di routing sono:

- *semplicità* dell'algoritmo, poiché i router hanno CPU e memoria finite e devono impiegare la maggior parte del loro tempo a instradare pacchetti, non a calcolare nuove tabelle di instradamento;
- *robustezza* e adattabilità alle variazioni di topologia; non deve esistere nessun presupposto né vincolo sulla topologia di rete, che deve poter essere modificata dinamicamente senza interrompere il funzionamento della rete;
- *ottimalità* nella scelta dei cammini, rispetto soprattutto ai due criteri elencati precedentemente;

- *stabilità*: a fronte di una rete stabile l'algoritmo deve sempre convergere velocemente ad un instradamento stabile, cioè non deve modificare le tabelle di instradamento se non a fronte di una variazione di topologia;
- *equità*: nessun nodo deve essere privilegiato o danneggiato.

Gli algoritmi di routing si dividono in due gruppi: *non adattativi* (statici e deterministici) e *adattativi* (dinamici e non deterministici). I primi utilizzano criteri fissi di instradamento, mentre gli altri calcolano le tabelle di instradamento in funzione della topologia della rete e dello stato dei link.

Sono algoritmi del primo gruppo il *fixed directory routing* e il *flooding*, mentre appartengono al secondo gruppo il *routing centralizzato*, il *routing isolato* e il *routing distribuito*.

Entrambi i gruppi hanno la loro ragione di esistere, in zone diverse della rete, come evidenziato in figura 14.5. Infatti, se per sfruttare al meglio le magliature della rete è indispensabile avere algoritmi di routing dinamico, nelle zone più periferiche della rete con topologia ad albero, cioè con un solo cammino che le interconnette al resto della rete, un routing statico può risultare più semplice e non presentare svantaggi.

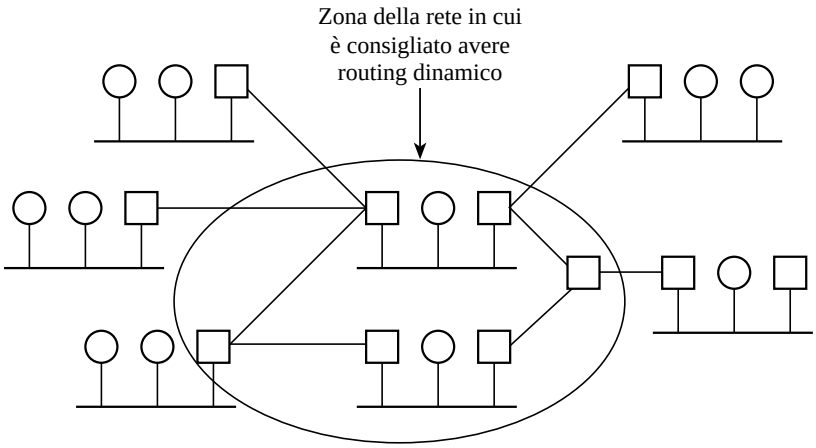


Fig. 14.5 - Routing statico e dinamico.

Gli algoritmi di più moderna concezione sono quelli distribuiti, che si suddividono ulteriormente in due famiglie: *distance vector* e *link state packet*.

14.4 ALGORITMI STATICI

14.4.1 Fixed directory routing

Il fixed directory routing prevede che ogni nodo abbia una tabella di instradamento che metta in corrispondenza il nodo da raggiungere con la linea da usare, e che tale tabella sia scritta manualmente dal gestore della rete nel router tramite un'operazione di management.

Il gestore ha il totale controllo dei flussi di traffico sulla rete, ma è necessario un suo intervento manuale per il reinstradamento di detti flussi in presenza di guasti. Questo approccio è spesso utilizzato in TCP/IP per le parti non magliate della rete e le regole di instradamento specificate su ogni singolo router prendono il nome di *route statiche*.

Esiste una variante, detta quasi-statica, che adotta tabelle con più alternative da scegliere secondo un certo ordine di priorità, in funzione dello stato della rete. Questo approccio, che consente di avere cammini alternativi in caso di guasto, è adottato, ad esempio, dalla rete SNA.

Occorre comunque evidenziare che la gestione manuale delle tabelle risulta molto complessa e difficoltosa, soprattutto per reti di grandi dimensioni.

In figura 14.6 vediamo un esempio di tabella di instradamento per fixed directory routing, che fornisce due scelte possibili: per ragioni esemplificative, al posto dell'indirizzo vi è un nome simbolico, poiché il formato dell'indirizzo può variare molto secondo il tipo rete considerata.

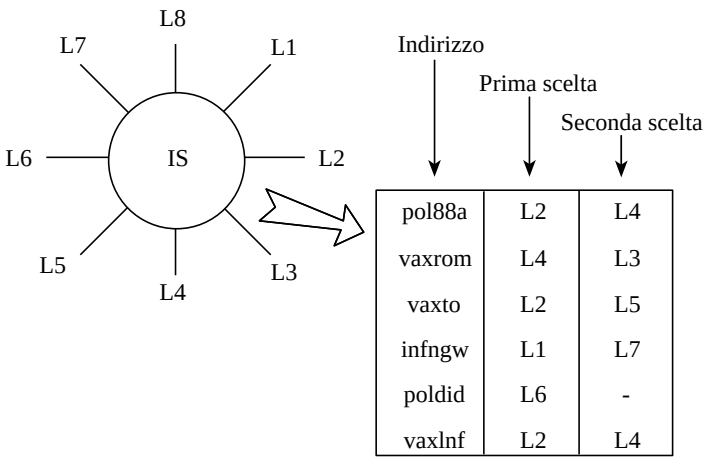


Fig. 14.6 - Esempio di fixed directory routing.

14.4.2 Flooding

Il flooding è un altro algoritmo non adattativo, in cui ciascun pacchetto in arrivo viene ritrasmesso su tutte le linee, eccetto quella su cui è stato ricevuto.

Concepito per reti militari a prova di sabotaggio, se realizzato nel modo sopra descritto massimizza la probabilità che il pacchetto arrivi a destinazione, ma induce un carico elevatissimo sulla rete.

Si può cercare di ridurre il carico utilizzando tecniche di *selective flooding*, in cui i pacchetti vengono ritrasmessi solo su linee selezionate.

Un primo esempio, senza applicazioni pratiche, è l'algoritmo *random walk* che sceglie in modo pseudo-casuale su quali linee ritrasmettere il pacchetto.

Una miglioria più efficace si ha scartando i pacchetti troppo vecchi, cioè quelli che hanno attraversato molti router: a tal scopo nell'header del pacchetto viene inserito un age-counter.

Un'ultima miglioria, ancora più significativa, consiste nello scartare un pacchetto la seconda volta che passa in un nodo: in tal modo si realizza una tecnica per trasmettere efficientemente la stessa informazione a tutti i nodi, qualsiasi sia la topologia. Lo svantaggio è che bisogna memorizzare tutti i pacchetti su ogni nodo per poter verificare se sono già passati.

Una tecnica di selective flooding è utilizzata per il calcolo delle tabelle di instradamento dal protocollo IS-IS (ISO 10598).

14.5 ALGORITMI ADATTATIVI

Gli algoritmi di instradamento adattativi sono quelli in cui le tabelle dipendono dalle informazioni raccolte sulla topologia della rete, sul costo dei cammini e sullo stato degli elementi che la compongono.

Gli algoritmi adattativi possono essere centralizzati (in un unico punto della rete vengono raccolte e analizzate tutte le informazioni, e calcolate le tabelle), isolati (ogni router è indipendente dagli altri) o distribuiti (i router cooperano al calcolo delle tabelle).

14.5.1 Routing centralizzato

Il routing centralizzato è tra i metodi adattativi quello che più si avvicina al fixed directory routing. Presuppone l'esistenza di un RCC (*Routing Control Center*) che conosce la topologia della rete, riceve da tutti i nodi informazione sul loro stato e su quello dei collegamenti, calcola le tabelle di instradamento e le distribuisce.

È un metodo che consente una gestione della rete molto accurata, in quanto permette di calcolare le tabelle anche con algoritmi molto sofisticati, ma implica l'esistenza di un unico gestore, ipotesi questa oggi molto spesso non realistica.

Il RCC, per ragioni di affidabilità, deve essere duplicato e la porzione di rete intorno ad esso è soggetta ad un elevato volume di traffico di servizio: informazioni di stato che arrivano al RCC e tabelle di instradamento che escono dal RCC.

In caso di guasti gravi possono verificarsi situazioni in cui il RCC perde il contatto con una parte periferica della rete e si verificano quindi degli aggiornamenti parziali di tabelle che possono determinare situazioni di loop.

Questo metodo è usato con successo nella rete TymNet, che è un'importante rete X.25 internazionale.

14.5.2 Routing isolato

Il routing isolato è l'opposto di quello centralizzato, visto che non solo non esiste un RCC, ma ogni IS si calcola in modo indipendente le tabelle di instradamento senza scambiare informazioni con gli altri IS.

Esistono due algoritmi di routing isolato riportati in letteratura: *hot potato* e *backward learning.*

Il primo è famoso solo per il suo nome simpatico (*hot potato*). Ogni IS considera un pacchetto ricevuto come una patata bollente e cerca di liberarsene nel minor tempo possibile, ritrasmettendo il pacchetto sulla linea con la coda di trasmissione più breve.

Il metodo di *backward learning* è invece utilizzato per calcolare le tabelle di instradamento nei bridge conformi allo standard IEEE 802.1D (si veda paragrafo 10.6). L'IS acquisisce una conoscenza indiretta della rete analizzando il traffico che lo attraversa: se riceve un pacchetto proveniente dal nodo A sulla linea L3, il backward learning impara che A è raggiungibile attraverso la linea L3.

È possibile migliorare il backward learning inserendo nell'header del pacchetto un campo di costo inizializzato a zero dalla stazione mittente ed incrementato ad ogni attraversamento di un IS. In tale modo gli IS possono mantenere più alternative per ogni destinazione, ordinate per costo crescente.

Tale situazione è mostrata in figura 14.7 in cui l'IS mantiene due alternative (entry) per ogni destinazione nella tabella di instradamento. Quando da *vaxrom* giunge un pacchetto con costo 6, la riga relativa a vaxrom viene aggiornata in quanto si è scoperto un cammino più conveniente di uno già noto.

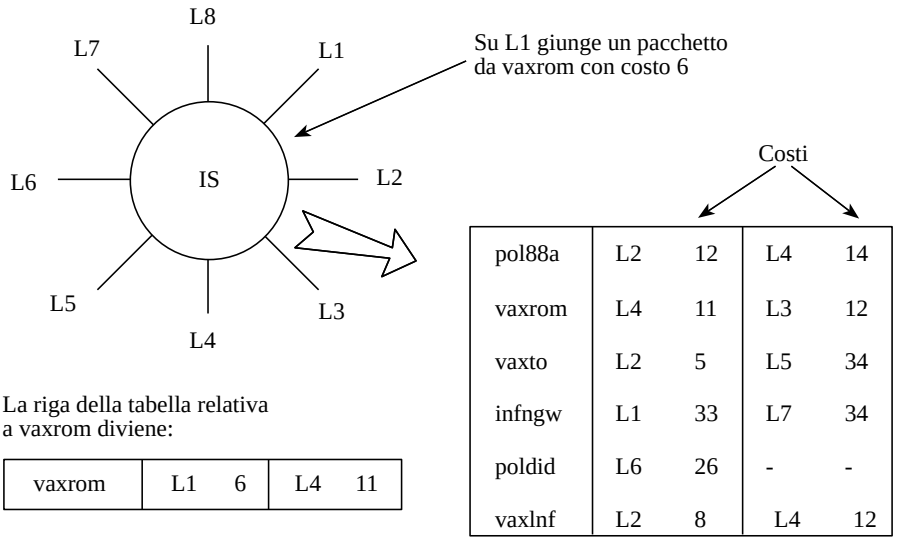


Fig. 14.7 - Esempio di routing isolato.

Il limite di questo metodo consiste nel fatto che gli IS imparano solo le migliorie e non i peggioramenti nello stato della rete: infatti se cade un link e si interrompe un cammino, semplicemente non arrivano più pacchetti da quel cammino, ma non giunge all'IS nessuna informazione che il cammino non è più disponibile.

Per tale ragione occorre limitare temporalmente la validità delle informazioni presenti nelle tabelle di instradamento: ad ogni entry viene associata una validità temporale che viene inizializzata ad un dato valore ogni volta che un pacchetto in transito conferma l'entry, e decrementata automaticamente con il passare del tempo. Quando la validità temporale di un'entry giunge a zero, questa viene invalidata ed eliminata dalla tabella di instradamento.

Qualora ad un IS giunga un pacchetto per una destinazione ignota, l'IS ne fa il flooding.

Il backward learning può generare loop su topologie magliate, per cui, ad esempio nei bridge, lo si integra con l'algoritmo di spanning tree per ridurre la topologia magliata ad un albero (si veda paragrafo 10.18).

14.5.3 Routing distribuito

Il routing distribuito è indubbiamente quello di maggior interesse per la soluzione dei problemi di internetworking. Esso si pone come una scelta di compromesso tra i

due precedenti: non esiste un RCC, ma le sue funzionalità sono realizzate in modo distribuito da tutti gli IS della rete, che a tal scopo usano un protocollo di servizio per scambiare informazioni tra loro ed un secondo protocollo di servizio per scambiare informazioni con gli ES. Tali protocolli vengono detti di servizio in quanto non veicolano dati di utente, che sono gestiti da un terzo protocollo, ma solo informazioni utili al calcolo delle tabelle di instradamento e al neighbor greetings.

Le tabelle di instradamento vengono calcolate a partire dai due parametri di ottimalità precedentemente descritti: costo e hop. Il costo di ciascuna linea di ciascun router è un parametro che viene impostato dal network manager tramite il software di gestione dei router stessi.

Gli algoritmi di routing distribuito sono oggi adottati da DECnet, TCP/IP, OSI, APPN, ecc., e si suddividono ulteriormente in due famiglie: algoritmi distance vector e algoritmi link state packet. Vista l'importanza di tali algoritmi, essi vengono descritti nei due appositi paragrafi che seguono.

14.6 ALGORITMI DI ROUTING DISTANCE VECTOR

L'algoritmo distance vector è anche noto come algoritmo di Bellman-Ford. Per realizzare tale algoritmo ogni router mantiene, oltre alla tabella di instradamento, una struttura dati, detta *distance vector* per ogni linea. Il distance vector associato a ciascuna linea contiene informazioni ricavate dalla tabella di instradamento del router collegato all'altro estremo della linea (si veda figura 14.8).

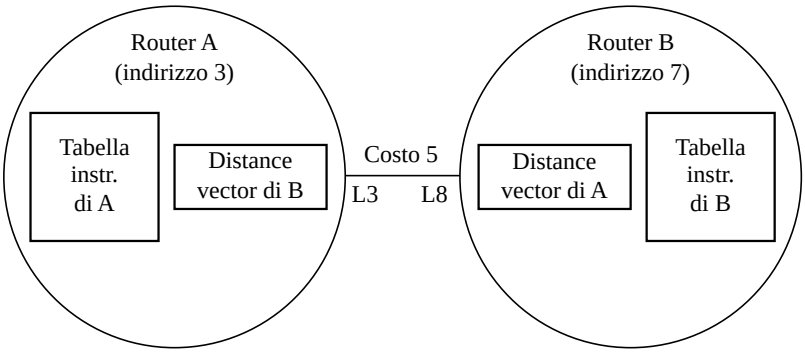


Fig. 14.8 - Router distance vector.

Il calcolo delle tabelle di instradamento avviene tramite un processo di fusione (merge) di tutti i distance vector associati alle linee attive di un router. Tutte le volte

che un router calcola una nuova tabella di instradamento, la invia agli IS adiacenti sotto forma di distance vector.

La tabella di instradamento è un insieme di quadruplette {indirizzo, hop, costo, linea} che contiene per ogni nodo della rete (indirizzo), sia esso un IS o un ES, l'informazione relativa al cammino migliore per raggiungere tale nodo in termini di numero di IS da attraversare (hop), somma dei costi delle linee da attraversare (costo) e linea su cui ritrasmettere il messaggio (linea). In figura 14.9 è riportata la tabella di instradamento del router A dell'esempio precedente.

Indirizzo	Hops	Costo	Linea
1	5	25	3
2	3	20	2
3	0	0	0
4	2	15	3
5	7	55	1
6	4	23	1
7	1	5	3
...	...	...	...

Fig. 14.9 - Tabella di instradamento di A.

Appare evidente che A ha indirizzo 3, in quanto esso appare raggiungibile in zero hop e con costo zero.

Ciascun router apprende tramite un protocollo di neighbor greetings (paragrafo 14.8) le informazioni relative ai nodi adiacenti, siano essi IS o ES, e le inserisce nella tabella di instradamento.

Quando un IS modifica la sua tabella di instradamento per una delle ragioni descritte nel seguito, esso invia a tutti gli IS adiacenti, cioè collegati da un cammino fisico diretto (solo a quelli adiacenti, non a tutti gli IS della rete) il suo distance vector che ricava dalle prime tre colonne della sua tabella di instradamento e che risulta quindi un insieme di triplette del tipo {indirizzo, hop, costo}. Un esempio di distance vector reale è riportato in appendice B, paragrafo B.4.4.

Quando un router riceve un distance vector da un router adiacente, prima di memorizzarlo, somma uno a tutti i campi hop e il costo della linea da cui ha ricevuto il distance vector a tutti i campi costo.

Nell'esempio precedente il router B che ha indirizzo 7, come appare evidente dalla tabella di instradamento di A, quando riceve il distance vector di A, gli aggiorna i campi hop e costo, e lo memorizza nella sua struttura dati locale come indicato in figura 14.10.

Indirizzo	Hops	Costo
1	6	30
2	4	25
3	1	5
4	3	20
5	8	60
6	5	28
7	2	10
...	...	...

Fig. 14.10 - Distance vector di A memorizzato in B.

Quando un router memorizza un distance vector nella sua struttura dati locale, verifica se sono presenti variazioni rispetto al distance vector precedentemente memorizzato: in caso affermativo ricalcola le tabelle di instradamento fondendo (*merge*) tutti i distance vector delle linee attive. Analoga operazione di ricalcolo avviene quando una linea passa dallo stato ON allo stato OFF o viceversa. Molte implementazioni ricalcolano anche le tabelle di instradamento periodicamente.

La fusione avviene secondo il criterio di convenienza del costo: a parità di costo secondo il minimo numero di hop e a parità di hop con scelta casuale. In figura 14.11 è riportato un esempio di calcolo della tabella di instradamento. La linea L0 indica il router stesso.

Se la tabella di instradamento risulta variata rispetto alla precedente, il distance vector relativo viene inviato ai router adiacenti. Alcune implementazioni di protocolli distance vector inviano anche i distance vector periodicamente, ad esempio il RIP (si veda il paragrafo 16.9.1) invia il distance vector ogni 30 secondi.

La modalità operativa descritta crea un fenomeno simile a quello di una pietra che cade in un catino di acqua. La pietra è una variazione dello stato della rete, il catino è la rete, le onde generate dalla caduta della pietra sono i distance vector che si dipartono dal luogo di impatto, arrivano ai bordi della rete, si specchiano e tornano verso il centro e ancora verso la periferia e poi verso il centro, con un moto che si ripete più volte prima di giungere a stabilità (acqua ferma).

Il vantaggio di questo algoritmo è la facilità di implementazione. Gli svantaggi sono:

- la complessità elevata, esponenziale nel caso peggiore e normalmente compresa tra $O(n^2)$ e $O(n^3)$. Questo rende improponibile l'utilizzo di tale algoritmo per reti con più di 1000 nodi, a meno che non venga adottato un partizionamento gerarchico come descritto in il paragrafo 14.9;

- la lenta convergenza ad un istradamento stabile. Infatti l'algoritmo converge con una velocità proporzionale a quella del link più lento e del router più lento presenti nella rete;
- la difficoltà di capirne e prevederne il comportamento su reti grandi, poiché nessun nodo ha la mappa della rete.

Questo algoritmo è usato in DECnet fase IV e in alcune realizzazioni TCP/IP (protocolli RIP e IGRP).

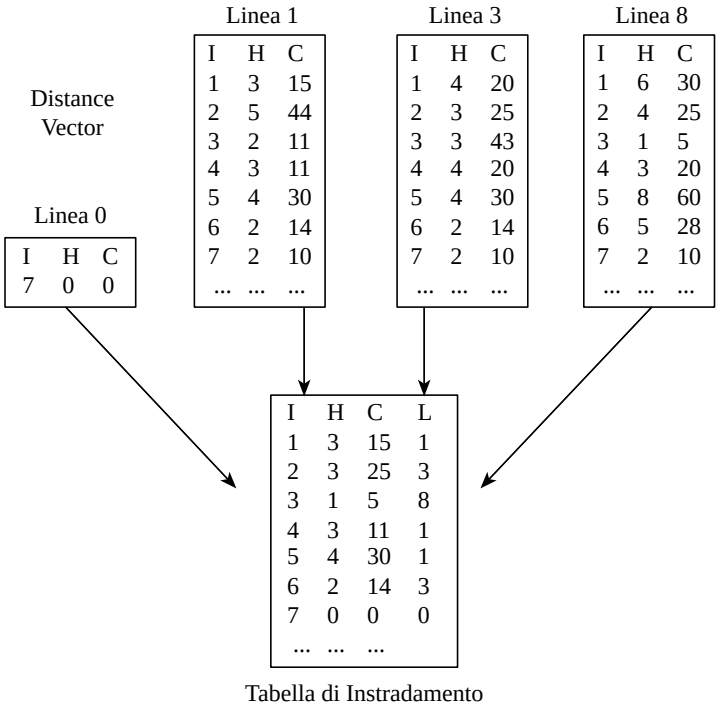


Fig. 14.11 - Funsione di distance vector in una tabella di instradamento.

14.7 ALGORITMI DI ROUTING LINK STATE PACKET

L'algoritmo link state packet assume che ogni IS disponga della mappa completa della rete su cui calcolare gli instradamenti ottimali utilizzando l'algoritmo di Dijkstra o *Shortest Path First* (SPF).

La mappa della rete non è scritta nei router dal sistema di gestione (sarebbe impraticabile per reti grandi), ma è costruita direttamente dai router tramite l'utilizzo

di *Link State Packet* (LSP).

Ogni router, tramite protocolli di neighbor greetings, apprende quali nodi sono a lui adiacenti e lo comunica agli altri router inviando un LSP che descrive tali adiacenze.

La figura 14.12 riporta un esempio di rete e del relativo LSP inviato dal router R1. Si noti che il LSP non contiene una entry per il router R4 in quanto non adiacente a R1.

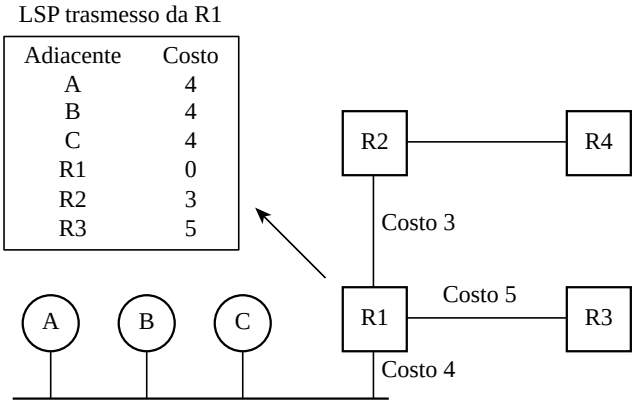


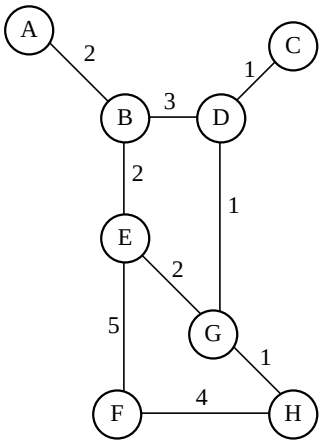
Fig. 14.12 - Trasmissione di LSP.

I Link State Packet sono trasmessi in selective flooding (si veda il paragrafo 14.4.2) a tutti gli IS della rete, secondo una modalità dettagliata nel seguito. Ogni IS contiene un LSP database in cui memorizza il LSP più recente generato da ogni IS.

Il LSP database è una rappresentazione del grafo della rete data come matrice delle adiacenze (si veda [1]). Si osservi che per definizione il LSP database deve essere esattamente lo stesso su tutti gli IS della rete. La figura 14.13 riporta un ipotetico grafo di rete, i cui vertici sono i nodi della rete (ES o IS) e i cui archi sono le linee con i costi associati, e il relativo LSP database.

Il LSP database, rappresentando la mappa della rete con i costi associati, è l'informazione necessaria e sufficiente affinché un router possa calcolare le sue tabelle di instradamento. Si noti la differenza con il distance vector: in quel caso i router cooperano direttamente per calcolare le tabelle di instradamento, qui i router cooperano per mantenere aggiornata la mappa della rete, poi ogni router calcola la propria tabella di instradamento in modo autonomo.

Il calcolo delle tabelle equivale al calcolo dello spanning tree di tipo Shortest Path First e si effettua con l'algoritmo di Dijkstra.



LSP Database

A	B/2		
B	A/2	D/3	E/2
C	D/1		
D	B/3	C/1	G/1
E	B/2	F/5	G/2
F	E/5	H/4	
G	D/1	E/2	H/1
H	F/4	G/1	

(replicato su ogni IS)

Fig. 14.13 - Grafo della rete e LSP database.

Ogni nodo ha a disposizione il grafo pesato della rete ed assegna a tutti gli altri nodi un'etichetta che rappresenta il costo massimo per la raggiungibilità del nodo in esame; l'algoritmo di calcolo modifica tali etichette cercando di minimizzarle e di renderle permanenti.

Le strutture dati coinvolte sono:

- l'insieme V dei vertici del grafo (i nodi della rete);
- il costo C [i, j] della connessione diretta da i a j (assunto infinito se tale connessione non esiste);
- il costo D[i] del cammino dal vertice 1 (assunto come radice dell'albero degli instradamenti, è cioè il nodo che sta effettuando il calcolo della tabella) al vertice i.

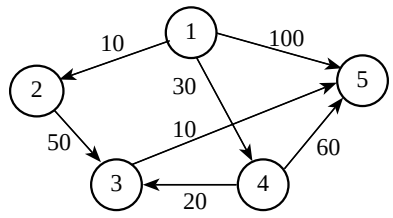
L'algoritmo inizializza $D[i]=C[1, i]$ e poi iterativamente cerca di minimizzare D[i], mantenendo un insieme S in cui memorizza quali vertici hanno già un valore definitivo (non ulteriormente riducibile).

La figura 14.14 riporta lo pseudo-codice dell'algoritmo e la figura 14.15 un esempio di applicazione.

```
procedure Dijkstra; {calcola il costo minimo tra tutti i cammini dal
    nodo 1 a tutti gli altri nodi}
begin
      S := {1};
      for i := 2 to n do D[i] := C[1,i]; {inizializza D}
      for i := 1 to n-1 do
      begin
            si scelga un nodo w in V-S tale che D[w] sia minimo;
            si aggiunga w a S;
            per ogni vertice v in V-S do D[v] := min(D[v], D[w] + C[w,v])
      end
end; {Dijkstra}
```

Fig. 14.14 - Algoritmo di Dijkstra.

L'applicazione dell'algoritmo di Dijkstra, all'esempio di figura 14.13, ad opera dell'IS B produce l'albero di instradamento di figura 14.16a, mentre quello ad opera dell'IS F produce l'albero di instradamento di figura 14.16b.



S	w	D[2]	D[3]	D[4]	D[5]
{1}	-	10	inf	30	100
{1,2}	2	10	60	30	100
{1,2,4}	4	10	50	30	90
{1,2,3,4}	3	10	50	30	60
{1,2,3,4,5}	5	10	50	30	60

Fig. 14.15 - Esempio di applicazione dell'algoritmo di Dijkstra.

I forwarding database risultanti, che verranno utilizzati dai router durante la normale operatività per inoltrare i pacchetti, sono riportati in figura 14.17.

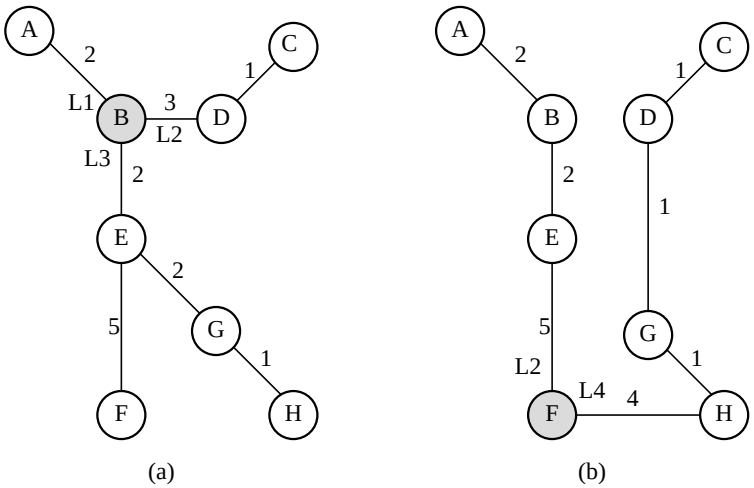


Fig. 14.16 - Alberi di instradamento.

Forwarding Table di B

A	L1
C	L2
D	L2
E	L3
F	L3
G	L3
H	L3

(a)

Forwarding Table di F

A	L2
B	L2
C	L4
D	L4
E	L2
G	L4
H	L4

(b)

Fig. 14.17 - Forwarding table.

La complessità dell'algoritmo link state packet è pari a L · log(N), dove L è il numero di link e N è il numero di nodi, ma poiché i costi dei link sono numeri interi piccoli, si riescono a realizzare strutture sofisticate che fanno tendere questo valore a N. Ad esempio, su un router da 1 MIPS inserito su una rete con 600 nodi e 300 link, il tempo di calcolo è di circa 150 ms.

Algoritmi di tipo link state packet sono utilizzati negli standard ISO 10589 (IS-IS) e nel protocollo OSPF (adottato in alcune reti TCP/IP).

L'algoritmo link state packet può gestire reti di grandi dimensioni (10000 nodi), ha convergenza rapida, difficilmente genera loop, e comunque è in grado di identificarli e interromperli facilmente, ed è facile da capire e prevedere poiché ogni nodo contiene l'intera mappa della rete.

Gli svantaggi sono invece nella difficoltà di programmazione e nella necessità di meccanismi speciali per gestire le LAN.

14.7.1 Architettura di un router LSP

Per meglio comprendere il funzionamento dell'algoritmo link state packet esaminiamo l'architettura di un router OSI CLNS che adotta l'algoritmo ISO 10589 (IS-IS), (figura 14.18).

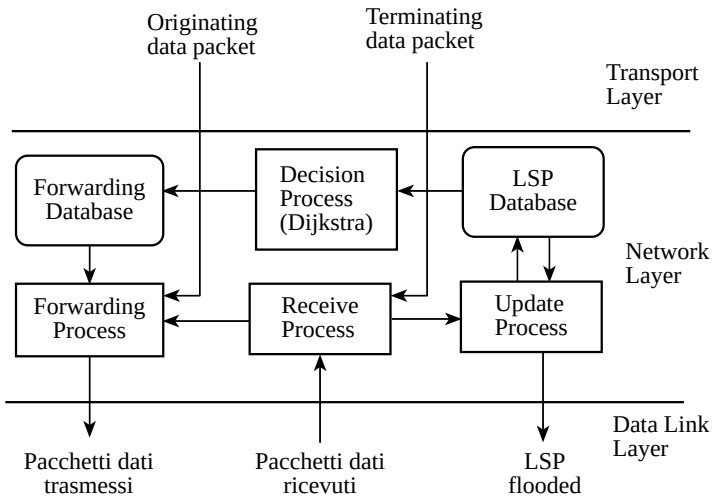


Fig. 14.18 - Architettura di un router LSP.

Quando il receive process riceve un pacchetto, verifica di quale tipo sia. Possono porsi tre casi:

- il pacchetto è un pacchetto dati in transito verso altre destinazioni; il receive process lo passa al forwarding process, che consulta il forwarding database usando come chiave l'indirizzo di destinazione e determina il nuovo instradamento, cioè su quale linea ritrasmettere il pacchetto;
- il pacchetto è un pacchetto dati destinato al router; ci troviamo in presenza di un pacchetto di gestione (management) che viene passato ai protocolli di livello superiore;
- il pacchetto è un LSP o un pacchetto di neighbor greetings; questo è il caso che necessita della trattazione più approfondita, riportata nel seguito.

Nel caso di un pacchetto di neighbor greetings il router verifica se si tratta di un nuovo nodo adiacente o di un nodo già noto. Nel secondo caso non fa nulla, nel primo caso genera un LSP per informare dell'esistenza del nuovo nodo tutti gli IS, in modo che il nuovo nodo diventi raggiungibile da qualsiasi punto della rete.

Un Link State Packet contiene, oltre alle informazioni di adiacenza già descritte, anche una checksum, un lifetime e un numero di sequenza che serve per distinguere, da parte di un router che riceve più LSP, quelli generati dallo stesso IS.

I LSP vengono trasmessi in flooding su tutti i link del router che li ha originati. Un router che riceve un LSP lo ritrasmette in flooding solo se esso ha modificato il LSP database del router stesso (selective flooding).

All'atto del ricevimento di un LSP un router compie le seguenti azioni:

- se non ha mai ricevuto LSP da quel mittente o se il numero di sequenza del LSP è maggiore di quello del LSP proveniente dalla stessa sorgente e memorizzato nel LSP database, allora memorizza il pacchetto nel LSP database e lo ritrasmette in flooding su tutte le linee eccetto quella da cui l'ha ricevuto;
- se il LSP ricevuto ha lo stesso numero di sequenza di quello posseduto, allora non occorre fare nulla poiché lo stesso pacchetto era già stato precedentemente trasmesso in flooding;
- se il LSP è più vecchio di quello posseduto, cioè è obsoleto, allora il router ricevente trasmette il LSP aggiornato al router mittente.

Questo meccanismo serve a fare in modo che i LSP database di tutti i router si mantengano perfettamente allineati e coerenti, condizione indispensabile per un corretto instradamento.

14.7.2 LSP e LAN

Le LAN sono strutture trasmissive broadcast che mal si prestano ad essere modellate come grafi. Infatti su una LAN tutti i nodi sono adiacenti a tutti gli altri e questo porterebbe ad un grafo completamente connesso con un numero di archi quadratico nel numero di nodi. Poiché il numero di nodi su una LAN può anche essere molto elevato tale approccio è improponibile oltre che inutile.

Per questo e per altri motivi si preferisce modellare la LAN come uno *pseudo-nodo*, un nodo fittizio non esistente sulla rete, che viene realizzato da uno dei router presenti sulla LAN (*designated router*): la topologia equivalente diventa dunque una stella con al centro lo pseudo-nodo.

La figura 14.19 mostra un esempio di LAN e il suo modello a stella mediante l'introduzione dello pseudo-nodo.

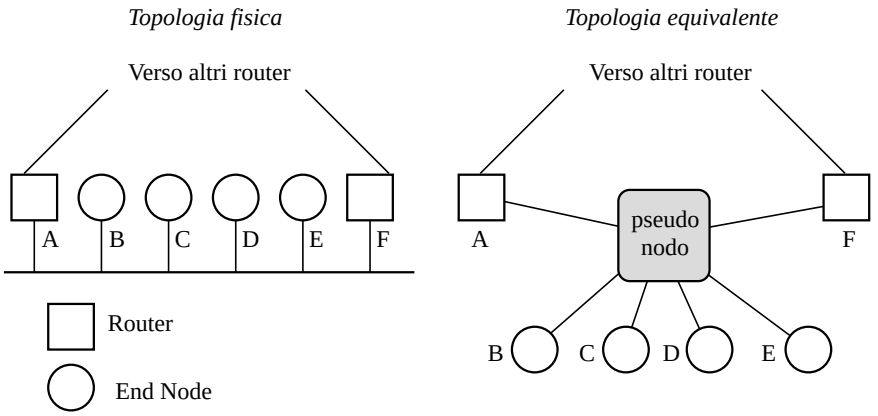


Fig. 14.19 - Lo pseudo-nodo.

Il calcolo delle tabelle di instradamento fatto sul modello a stella delle LAN è utile in quanto ogni ES vede la LAN come un collegamento punto-punto con lo pseudo-nodo e quindi non ha necessità di avere informazioni di routing in quanto, indipendentemente dalla destinazione con cui vuole comunicare, è sufficiente che l'ES invii i pacchetti allo pseudo-nodo. Chiaramente un approccio di questo genere risulta particolarmente inefficiente quando due nodi sulla stessa LAN vogliono comunicare, ma, integrato con la problematica del neighbor greetings, può essere la base su cui risolvere molti problemi.

14.8 NEIGHBOR GREETINGS

Per la gestione delle interazioni tra ES e IS su rete locale esiste un protocollo apposito che secondo la terminologia OSI si chiama ES-IS (*End System to Intermediate System*).

Tale protocollo ha due scopi:

- Permettere agli ES di conoscere gli IS presenti sulla LAN e viceversa. Questo viene realizzato con la trasmissione periodica in multicast di tipo advertisement di due pacchetti: gli ISH (*Intermediate System Hello*) e gli ESH (*End System Hello*). Gli ISH sono trasmessi dai router e ricevuti da tutti gli ES che memorizzano, in questo modo, l'esistenza di un IS in una cache locale. Gli ESH sono trasmessi dagli ES e ricevuti dagli IS che, in questo modo, scoprono le adiacenze da includersi nei LSP.

- Permettere agli ES di apprendere tramite pacchetti di *routing redirect* se un nodo è direttamente collegato alla LAN oppure qual è il miglior router tramite il quale raggiungerlo.

La figura 14.20 evidenzia i tre tipi di pacchetti e la loro direzione.

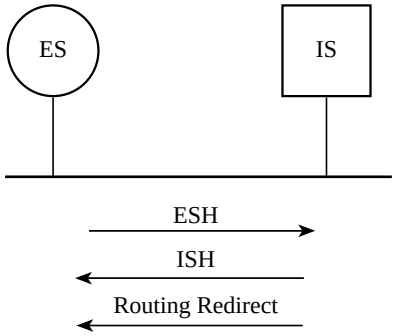


Fig. 14.20 - Neighbor greetings.

Quando un ES deve trasmettere un pacchetto ad un altro ES può ignorare dove si trovi l'ES destinatario ed inviare il pacchetto allo pseudo-nodo, ad un IS sulla sua LAN o al suo router di default (dipende dalle architetture di rete). A ricevere il pacchetto sarà comunque sempre un router che, se verifica che il pacchetto deve essere ritrasmesso sulla stessa LAN da cui è stato ricevuto, genera un pacchetto di routing redirect, oltre a recapitare comunque il pacchetto.

Il pacchetto di routing redirect indica all'ES l'esistenza di un cammino migliore per raggiungere la destinazione. Tale cammino può essere diretto nel caso che l'ES di destinazione si trovi sulla stessa LAN o indiretto se il pacchetto deve transitare per un altro router.

L'ES mittente, all'atto della ricezione di un pacchetto di routing redirect, impara l'informazione in esso contenuta e la scrive nella sua cache locale. I pacchetti successivi per lo stesso destinatario verranno inviati direttamente nel modo indicato dal contenuto del pacchetto di routing redirect.

Questo meccanismo è flessibile perché consente a tutti gli ES di comunicare nel modo ottimale con tutti gli altri nodi della rete (ad eccezione del primo pacchetto) ed inoltre limita la dimensione della cache sugli ES: infatti in essa sono contenuti solo gli indirizzi degli IS collegati alla LAN e la raggiungibilità degli ES con cui sono in corso scambi di informazioni.

14.9 ROUTING GERARCHICO

Anche se si adottano algoritmi di tipo LSP non è certo pensabile che essi riescano a trattare qualsiasi rete di qualsiasi dimensione: si pensi a Internet con le sue decine di milioni di calcolatori collegati e un tasso di crescita del 5% al mese.

Quindi occorre organizzare il routing in modo gerarchico, cioè partizionare la rete in aree (a volte si usano anche i termini di dominio, net o subnet). All'interno dell'area (routing intra-area) il routing segue esattamente le regole sin qui descritte. Quando invece bisogna far comunicare due nodi appartenenti ad aree diverse (routing inter-area) si divide il problema in tre sottoproblemi:

- un problema di instradamento tra il nodo mittente e la periferia dell'area cui il nodo mittente appartiene;
- un problema di instradamento tra l'area mittente e l'area destinazione;
- un problema di instradamento all'interno dell'area destinazione.

Tutte le principali architetture di rete attuali hanno il concetto di routing gerarchico. Ad esempio, SNA ha il concetto di subarea, OSI ha i concetti di dominio e area, DECnet quello di area, TCP/IP quello di network e subnetwork.

La figura 14.21 illustra una rete ripartita in tre aree. Supponiamo di dover instradare il messaggio dal nodo G al nodo A. In una prima fase si invia il messaggio ad F (router di area per l'area 15). F deve instradare il messaggio all'area 10 e ha due possibilità: il cammino diretto con costo 3 o quello indiretto con costo 4 (tramite l'area 12). Sceglie ovviamente il cammino diretto e passa il messaggio ad E, che lo passa a D, che lo passa a B che lo recapita ad A, nodo destinatario.

Si noti che l'instradamento ottenuto è ottimale, ma non ottimo: infatti il suo costo è pari a 16, mentre se si fosse passati da C il costo sarebbe stato pari a 10.

Questo è uno degli svantaggi del routing gerarchico in quanto, non avendo una visione globale della rete, si compiono tante scelte ottime di per sé, ma che considerate nell'insieme possono non rappresentare l'ottimo globale.

Il grande vantaggio del routing gerarchico è che ogni area ha dimensioni ragionevoli e può essere gestita da algoritmi di routing distribuito.

Si noti infine che nulla vieta di avere più livelli di gerarchia, cosa che avviene in OSI e TCP/IP.

Il routing gerarchico necessita di alcune cautele nella configurazione dei cammini inter-area. Per capire il problema si consideri la semplice rete riportata in figura 14.22.

In presenza del guasto indicato, il nodo 3.1 non riesce a scambiare messaggi con il nodo 5.2. Questo può essere compreso se si applica il criterio di instradamento inter-area prima discusso.

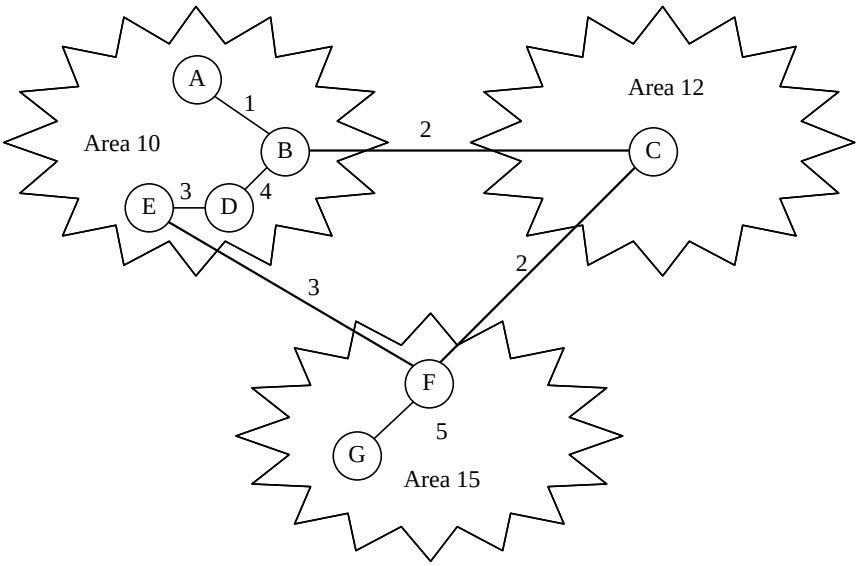


Fig. 14.21 - Routing gerarchico.

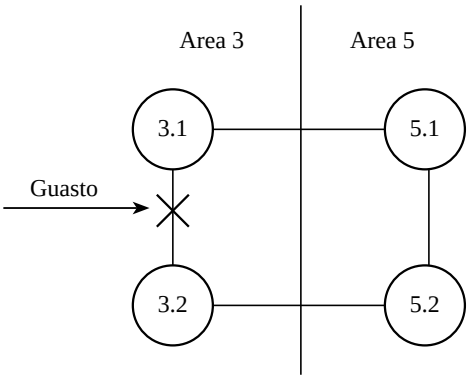


Fig. 14.22 - Area partizionata.

Infatti 3.1 cerca per prima cosa di far giungere il messaggio nell'area destinazione e quindi lo passa a 5.1 che, effettuando un instradamento intra-area, lo consegna al nodo 5.2. Il nodo 5.2, ai livelli superiori (tipicamente a livello trasporto), genera un acknowledge che viene instradato verso il nodo 3.1 a livello 3. Il nodo 5.2 cerca per prima cosa di inviare il messaggio all'area di destinazione e lo passa al nodo 3.2. Il

nodo 3.2 consulta le sue tabelle di instradamento, constata che non esiste un cammino intra-area con il nodo 3.1 e scarta il messaggio in quanto non recapitabile. Questo avviene perché l'area 3 è partizionata: è come se sulla rete esistessero due diverse aree 3, una raggiungibile tramite il nodo 5.1 e l'altra tramite il nodo 5.2.

Questo esempio ci permette di fare un'osservazione importante: quando si usano protocolli di livello 3 connectionless con routing distribuito non si è certi che il messaggio da A a B faccia lo stesso percorso del messaggio da B ad A. Occorre quindi configurare le aree in modo fortemente connesso, in modo che la caduta di un solo link non possa portare al loro partizionamento. È inoltre opportuno minimizzare i punti di contatto tra le aree cercando di renderli il più possibile affidabili.

Sempre con riferimento alla figura 14.22, si noti che se a guastarsi fosse stato il link tra 3.2 e 5.2 invece di quello tra 3.1 e 3.2, nessuna area si sarebbe partizionata e la rete avrebbe continuato a funzionare correttamente.

BIBLIOGRAFIA

[1] J. V. Aho, J. E. Hopcroft, J. D. Ullman, "Data Structures and Algorithms", Addison-Wesley, Reading MA (USA), 1983.

[2] Cisco Systems, "Internetworking Technology Overview", Codice documento DOC-ITO13 78-1070-01, 1993.

[3] A. Tanenbaum, "Computer Networks," Prentice-Hall.

[4] J. Martin, J. Leben, "DECnet Phase V: An OSI Implementation", Digital Press, Bedford MA (USA), 1992.

[5] ISO 8802-2 (ANSI/IEEE Std 802.2), "Logical Link Control".

[6] Cisco Systems, "Router Products Configuration and Reference", Cisco Systems DOC-R9.1, Menlo Park CA (USA), September 1992.

[7] ISO, "TR 9577: Information technology - Telecommunications and information exchange between systems - Protocol identification in the OSI network layer", 1990.

[8] ISO, "DTR 9577: Information technology - Telecommunications and information exchange between systems - Protocol identification in the OSI network layer", 1993.

[9] ISO 8473, "Protocol for Providing the Connectionless-mode Network Service".

[10] ISP 9542, "End system to Intermediate system routeing exchange protocol for

use in conjunction with the Protocol for providing the connectionless-mode network service".

[11] ISP 10589, "Intermediate system to Intermediate system Intra-Domain routeing information exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service".

[12] J. Postel, "RFC 791, Internet Protocol", 09/01/1981.

[13] J. Postel, "RFC 792: Internet Control Message Protocol", 09/01/1981.

[14] C. Hedrick, "RFC 1058, RIP: Routing Information Protocol", 06/01/1988.

[15] G. Malkin, "RFC 1388: RIP Version 2 Carrying Additional Information", 01/06/1993.

[16] J. Moy, "RFC 1583: OSPF Version 2", 03/23/1994. (Pages=212).

[17] K. Lougheed, Y. Rekhter, "RFC 1267: A Border Gateway Protocol 3 (BGP-3)", 10/25/1991.

[18] M. L. Peters, "APPN and Extensions: The New Industry Standard for SNA Internetworking", IBM Corp, Research Triangle Park, NC, USA.

[19] J. P. Graym Marcia L. Peters, "A Preview of APPN High Performance Routing", IBM Corp, Research Triangle Park, NC, USA, July 1993.

15

L'ARCHITETTURA DI RETE DNA/DECNET

15.1 INTRODUZIONE

DNA (Digital Network Architecture) è l'architettura di rete della DEC (Digital Equipment Corporation). Si tratta di un'architettura di rete proprietaria, con aperture verso gli standard, i cui protocolli sono realizzati sia da DEC sia da molti altri costruttori di calcolatori e apparati di routing.

DECnet è il nome della principale famiglia di prodotti hardware e software che realizzano DNA. DECnet è nata nel 1975 come mezzo per far comunicare tra loro calcolatori di tipo PDP-11 e si è evoluta attraverso tre versioni principali dette *fasi*.

DECnet fase III è stata la prima versione ad avere un successo commerciale, ma è stata DECnet fase IV, introdotta parallelamente ai calcolatori VAX e al sistema operativo VMS, a dare a DECnet la grande diffusione. Oggi la maggior parte dei calcolatori che fa parte di una rete conforme a DNA utilizza DECnet fase IV.

La rete DECnet è stata concepita sin dall'inizio come una rete di calcolatori paritetici che possono comunicare con qualsiasi altro calcolatore senza che i messaggi debbano transitare attraverso un calcolatore centrale. Il software DECnet è stato progettato pensando alle problematiche di *distributed processing* e l'hardware ha utilizzato le reti locali ed in particolare Ethernet sin dalla loro nascita.

La struttura di una rete DECnet è quindi quella di una interconnessione di reti locali Ethernet tramite router che implementano i primi tre livelli dell'architettura DECnet. Quindi DECnet ha precorso i tempi e ha concepito la rete globale come un internetworking di LAN.

I protocolli di DECnet fase IV, pur essendo simili a quelli di OSI, non sono compatibili con questi ultimi, né lo sono con quelli dell'architettura TCP/IP. Fase IV è quindi una architettura proprietaria, molto diffusa anche su calcolatori non DEC e

che ha dei limiti nelle dimensioni massime delle reti che si possono realizzare (circa 64000 nodi) a causa di un indirizzamento limitato a 16 bit. Per questa ragione dal 1991 DEC ha introdotto DECnet fase V.

DECnet fase V è un'architettura di rete totalmente compatibile con gli standard OSI e per questo viene spesso detta anche DECnet/OSI. DEC è stato il primo costruttore di calcolatori ad abbandonare un'architettura di rete proprietaria per adottare lo standard OSI. Altri costruttori di calcolatori hanno deciso di abbandonare le loro reti proprietarie, ma di adottare lo standard "de facto" TCP/IP. Visto il grande successo di mercato e la grande diffusione dell'architettura TCP/IP e di Internet anche DEC ha prodotto una nuova versione di DECnet (DECnet fase IP) che appoggia gli applicativi proprietari di DECNET fase IV sull'architettura TCP/IP.

DECnet fase V, oltre ad essere compatibile con OSI, mantiene anche la compatibilità con DECnet fase IV e permette di realizzare reti miste in cui alcuni calcolatori utilizzano il software fase IV, altri quello fase V.

Realizzazioni di DECnet sono oggi disponibili su moltissime piattaforme, a partire dal personal computer sino al mainframe.

15.2 DECNET FASE IV

15.2.1 Nodi, linee e circuiti

Nodi, linee e circuiti sono i tre elementi base che costituiscono una rete DECnet fase IV (detta da qui in poi semplicemente DECnet).

I *nodi* sono i calcolatori, i router o i gateway, cioè tutti quegli elementi di rete che realizzano il livello 3 di DECnet (*routing*) e che hanno quindi un indirizzo DECnet. L'indirizzo deve essere univoco su tutta la rete.

All'indirizzo è molto spesso associato, per comodità, un nome tramite una base di dati locale a ciascun nodo e quindi non è né garantita né richiesta la consistenza dei nomi sulla rete.

I nodi sono interconnessi tramite *linee* che possono essere di tipo punto-punto, punto-multipunto o broadcast (le reti locali). Sulle linee fisiche si definiscono canali logici di comunicazione detti *circuiti*. I circuiti sono i mezzi con cui i nodi si scambiano i pacchetti DECnet. La distinzione tra linee e circuiti è poco significativa sui canali punto-punto o sulle rete locali, in cui è associato un circuito per ogni linea, ma è più importante per le linee punto-multipunto o per le reti a commutazione di pacchetto (ad esempio X.25) in cui su un'unica linea è possibile definire più circuiti.

La figura 15.1 mostra un esempio in cui la linea 2 interconnette in modalità

punto-multipunto i nodi B, C e D, e sono definiti su di essa due circuiti, uno tra B e C e l'altro tra B e D.

Poiché un calcolatore può eseguire contemporaneamente più programmi e processi, è indispensabile stabilire un collegamento tra due processi che comunicano utilizzando la rete: tale connessione logica in DECnet si chiama *logical link*. Il programma o processo con cui un altro programma o processo chiede di stabilire un logical link è detto *object.*

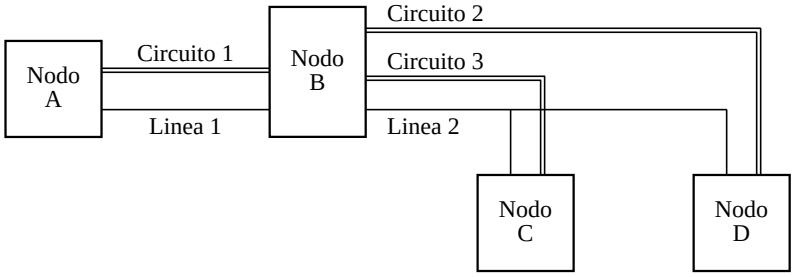


Fig. 15.1 - Nodi, linee e circuiti.

Un logical link può essere definito tra due processi in esecuzione sullo stesso calcolatore o su calcolatori vicini, ma anche tra due processi localizzati su calcolatori molto distanti. In questo caso i pacchetti inviati sul logical link attraversano molti nodi intermedi prima di giungere a destinazione e i nodi intermedi provvedono al loro instradamento utilizzando la funzionalità di routing.

15.2.2 Architettura a livelli

La figura 15.2 mostra affiancati il modello di riferimento OSI, l'architettura di DECnet e alcuni protocolli utilizzati in DECnet.

Si noti che la struttura di DECnet è molto simile a quella di OSI in quanto deriva dallo stesso "ceppo", ma è incompatibile con quest'ultima in quanto i protocolli utilizzati da DECnet non sono conformi agli standard OSI.

In particolare, a livello 1 (Fisico) e 2 (Data Link) DECnet può utilizzare canali punto-punto o punto-multipunto gestendoli con il protocollo proprietario DDCMP (*Digital Data Communication Message Protocol*), reti locali (Ethernet e FDDI), reti a commutazione di pacchetto (X.25) e il bus CI (*Computer Interconnect*), un bus seriale a 70Mb/s utilizzato da DEC per la sua architettura cluster.

Il DDCMP è un protocollo di tipo *byte-oriented*, proprietario, progettato nel 1974 espressamente per la rete DECnet. Pur avendo buone prestazioni è un protocollo superato in quanto oggi si utilizzano esclusivamente protocolli della famiglia HDLC, previsti negli standard OSI.

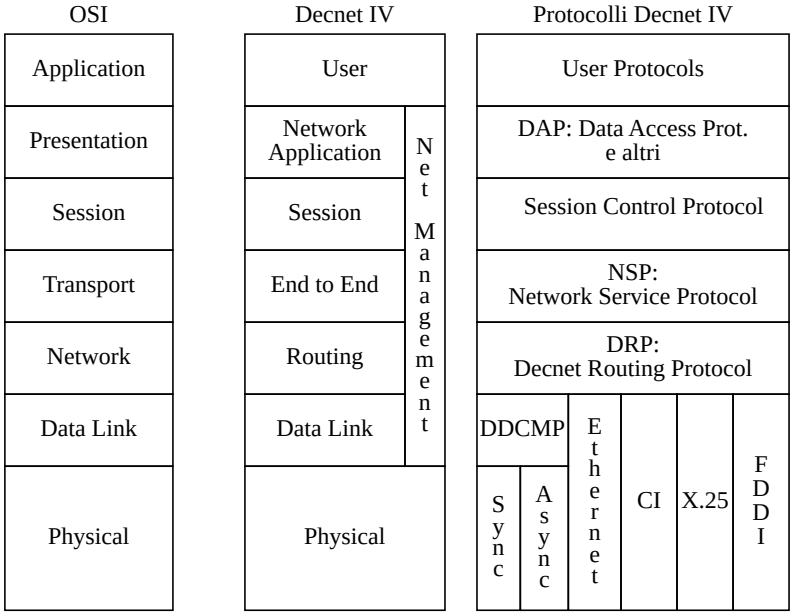


Fig. 15.2 - Architettura di DECnet fase IV.

L'interconnessione alle reti locali avviene tramite Ethernet v.2.0 (non IEEE 802.3) e FDDI. Questo non significa che non si possa utilizzare hardware conforme ad IEEE 802.3, ma solo che l'imbustamento utilizzato è quello Ethernet v.2.0.

Reti locali Ethernet e FDDI su cui sono utilizzati protocolli DECnet possono essere interconnesse tramite router o bridge.

Le reti a commutazione di pacchetto X.25 sono viste come canali punto-multipunto su cui realizzare uno o più circuiti DECnet detti DLM (*Data Link Mapping*), verso altrettanti DTE X.25. I DLM devono essere predefiniti in modo consistente sui router che li gestiscono.

A livello 3 (routing) DECnet utilizza il protocollo non connesso DRP (*DECnet Routing Protocol*) e un routing di tipo adattativo, dinamico, basato su un algoritmo distance vector (si veda paragrafo 14.6). Le decisioni di routing di DECnet sono basate sui concetti di costo e di hop.

Per ogni logical link, DECnet cerca di determinare un cammino di instradamento detto *path* che minimizzi il costo e, a parità di costo, il numero di hop. Se due oggetti X e Y devono comunicare esistono due path, uno che collega X a Y e l'altro che collega Y a X. Generalmente i due path sono diversi.

Se un path diventa non più disponibile a causa di un guasto, i router determinano immediatamente se esiste un path alternativo e in questo caso reinstradano il logical link sul nuovo path senza che questo cada e debba essere riattivato.

La figura 15.3 mostra i moduli hardware e software che normalmente sono presenti su un nodo DECnet con una visione complementare a quella di figura 15.2. Si noti il modulo DRP (modulo di routing) che concentra e smista tutte le comunicazioni che giungono dai vari circuiti e dal software di livello superiore.

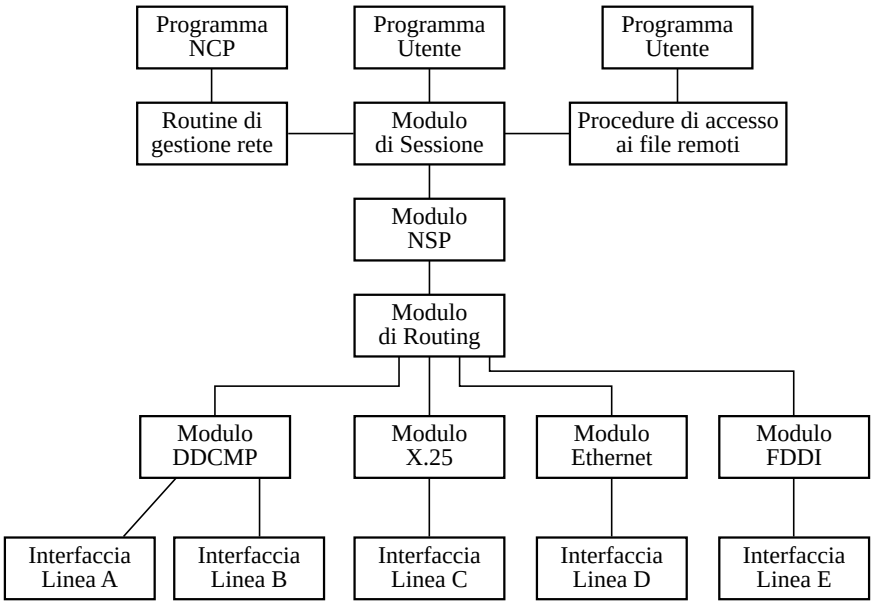


Fig. 15.3 - Moduli DNA su un nodo DECnet.

Il modulo DRP è di tipo connectionless e quindi tratta i pacchetti secondo la filosofia datagram. Per rendere affidabile la comunicazione sul modulo DRP si appoggia il modulo NSP (*Network Service Protocol*) che include anche le funzionalità di gestore delle connessioni, controllo di flusso, controllo degli errori, segmentazione e riassemblaggio dei messaggi. Il modulo NSP ha funzionalità simili al TP4 OSI.

Sul modulo NSP si appoggia il Session Control Layer che definisce gli aspetti della comunicazione che dipendono dai sistemi, quali la traduzione da nomi ad

indirizzi, l'indirizzamento dei processi e il controllo degli accessi.

Sul modulo di *session control* possono appoggiarsi gli applicativi di utente, sia indirettamente, utilizzando ad esempio delle procedure di accesso a file remoti (DAP), sia direttamente. Infine sul session control si appoggiano i moduli di network management.

Un esempio di pacchetto DAP è riportato in appendice B, paragrafo B.4.1.

15.2.3 Indirizzi

Gli indirizzi di DECnet sono su 16 bit (2 byte o 2 ottetti). I 16 bit sono divisi in due gruppi: un primo gruppo di 6 bit è detto indirizzo di area, un secondo gruppo di 10 bit è detto indirizzo di nodo. Gli indirizzi si scrivono in decimale con un punto tra i due gruppi, nella forma *Area.Nodo* (figura 15.4).

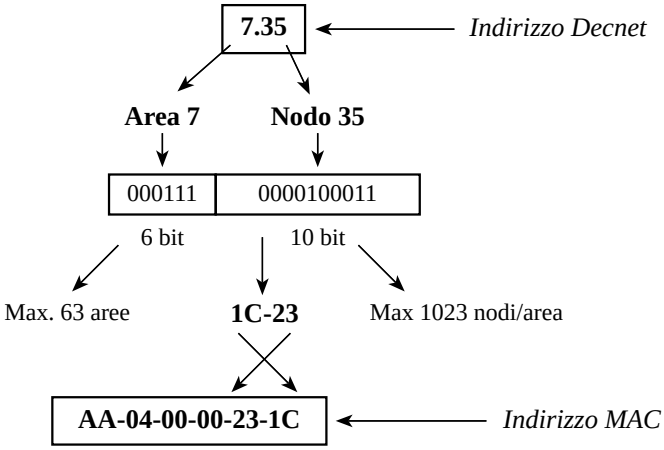


Fig. 15.4 - Indirizzi.

L'indirizzo 0.0 è riservato ed indica il calcolatore stesso, quindi il numero massimo di aree è 63 (da 1 a 63) e il numero massimo di nodi per area 1023 (da 1 a 1023). Esempi di indirizzi sono 2.1, 63.1023 e 7.19.

Lo spazio di indirizzamento di DECnet, grande circa 64000 nodi, pur non avendo una dimensione esigua, è troppo limitato per consentire un indirizzamento univoco a livello mondiale. Per questo motivo non è mai esistita una *addressing authority* internazionale per DECnet e quindi gli utenti hanno assegnato gli indirizzi in funzione di piani di indirizzamento interni alle varie organizzazioni.

La relazione tra gli indirizzi di livello 3 e gli indirizzi di livello 2 MAC è

algoritmica ed è riportata in figura 15.4. Il software DECnet, quando viene attivato su una scheda di rete locale, sostituisce all'indirizzo MAC *universal*, definito nella ROM della scheda, un indirizzo *local* ricavato preponendo ai 16 bit dell'indirizzo DECnet i seguenti 32 bit: AA-00-04-00 (per ulteriori dettagli si veda il paragrafo 5.6.7). In tal modo DECnet non necessita di protocolli ausiliari quali l'ARP di TCP/IP per mantenere una tabella di corrispondenza tra questi due tipi di indirizzi.

Si noti che DECnet, poiché cambia l'indirizzo MAC delle schede di LAN, deve essere il primo protocollo di rete ad essere attivato in un ambiente multiprotocollo. In caso contrario, un protocollo attivato prima del DECnet supporrebbe di utilizzare l'indirizzo MAC universal della scheda di LAN, invece di quello local forzato dal DECnet, e quindi non funzionerebbe.

15.2.4 Gerarchia

Il tipo di gerarchia realizzabile è esemplificata in figura 15.5. Essa mostra una rete gerarchica con tre aree DECnet, la 1, la 3 e la 6. Si noti che i nodi devono appartenere totalmente ad una sola area e quindi anche i router appartengono ad un'area, pur potendo gestire collegamenti con altre aree. Questo può sembrare banale, ma deve essere evidenziato in quanto un'altra importante architettura di rete (il TCP/IP) usa un approccio diverso.

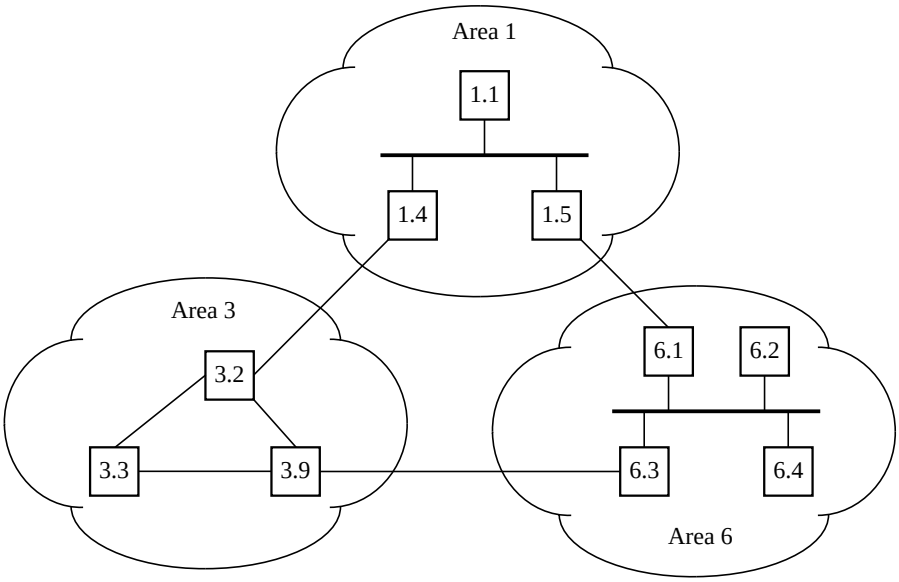


Fig. 15.5 - Struttura gerarchica.

I nodi che partecipano a questa struttura gerarchica si dividono in tre classi:

- *End Node* (EN): hanno un solo collegamento di rete con un altro nodo della stessa area;
- *Router di livello 1* (L1): hanno più di un collegamento di rete, ma tutti con nodi appartenenti alla stessa area;
- *Router di livello 2* (L2): hanno collegamenti anche con router di altre aree o comunque si trovano su un cammino tra aree diverse.

I router di livello 2 vengono anche detti *area router* e svolgono sempre anche le funzionalità di router di livello 1.

15.2.5 Router di livello 1 e 2

I router di livello 1 gestiscono collegamenti *intra-area,* cioè all'interno della stessa area, mentre i router di livello 2 gestiscono collegamenti *inter-area*.

La figura 15.6 mostra un esempio di rete con 2 aree e la tipologia dei nodi.

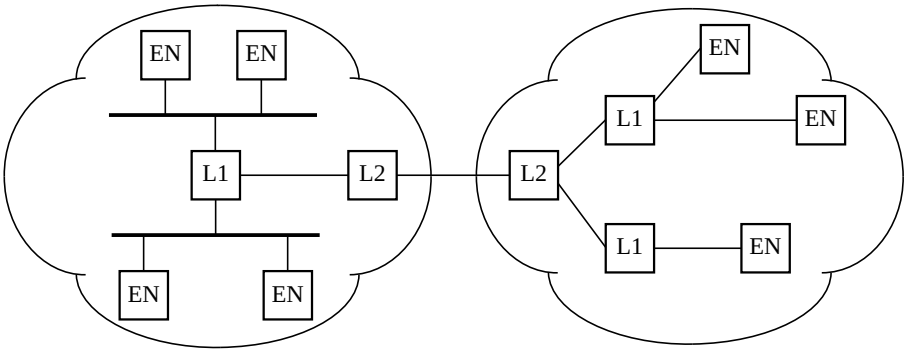


Fig. 15.6 - Router e End Node.

DECnet non impone alcuna relazione tra le aree e le reti fisiche. La figura 15.7 mostra tre possibili piani di indirizzamento per la stessa rete, tutti e tre leciti e funzionanti.

Un'area può corrispondere ad una LAN (figura 15.7b), ma più LAN possono far parte della stessa area (figura 15.7a), oppure più aree possono essere presenti sulla stessa LAN (figura 15.7c). Tuttavia questa estrema flessibilità di configurazione deve essere usata con "buon senso". È opinione degli autori che il buon senso debba sempre essere il primo criterio progettuale, ma l'esperienza quotidiana nella diagnosi delle reti malfunzionanti indica che così non è! In particolare occorre non dimenticare il

problema dell'area partizionata, illustrato nel paragrafo 14.9, cui DECnet è soggetta. Quindi è bene limitare il numero di connessioni inter-area. Una progettazione ideale da questo punto di vista consiste nel collegare tutti gli area router su un'unica LAN (Ethernet o FDDI) e gestire solo collegamenti geografici di tipo intra-area.

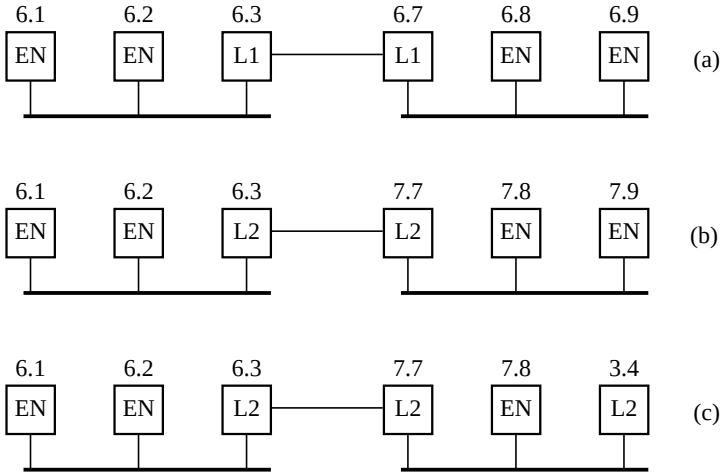


Fig. 15.7 - Aree e reti fisiche.

Quando questo approccio non è possibile, occorre almeno configurare le aree in modo magliato affinché un guasto singolo non le partizioni e comprendere quali router devono essere di livello 1 e quali di livello 2, tenendo conto che un nodo deve avere il minimo livello possibile per ottenere prestazioni elevate. È errato, ad esempio, definire un EN come L1, anche se la rete continua a funzionare.

La figura 15.8 mostra una rete con 3 aree e il livello appropriato dei nodi. Si noti che il router R27 deve essere di livello 2 anche se ha solo collegamenti intra-area.

Infatti R27 si trova su una maglia di livello 2 e in caso di guasti può trovarsi a dover trasportare traffico inter-area e comunque, anche in assenza di guasti, deve propagare i distance vector di area routing che si scambiano i router di livello 2.

L'appendice B riporta esempi di distance vector di livello 2 (paragrafo B.4.5) e di livello 1 (paragrafo B.4.4). Inoltre nei paragrafi B.4.2 e B.4.3 sono riportati i pacchetti di neighbor greetings che DECnet utilizza su LAN per permettere ai router di conoscere gli end node e viceversa.

Tramite i pacchetti di neighbor greetings DECnet elegge su ogni LAN un*designated router di livello 1* ed eventualmente un *designated router di livello 2*. Il ruolo del designated router è simile a quello dello pseudo-nodo introdotto nel paragrafo 14.7.2.

Il designated router riceve i pacchetti dagli end node e li instrada sulla rete inviando eventualmente messaggi di routing redirect ai nodi mittenti.

Il progetto di una rete DECnet si riduce quindi a tre semplici fasi:

- identificazione delle aree e stesura del piano di indirizzamento;
- assegnazione degli indirizzi a tutti i nodi;
- assegnazione del livello (EN, L1, L2) a tutti i nodi.

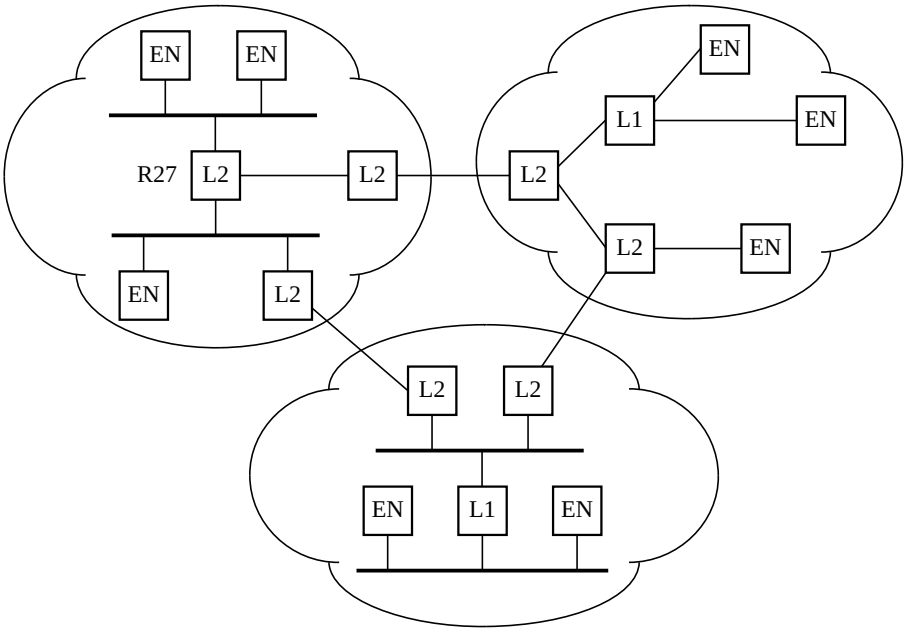


Fig. 15.8 - Router di livello 1 e 2.

Queste tre fasi portano ad una rete funzionante che può essere ottimizzata durante il normale funzionamento agendo sui costi delle linee e sull'elezione dei designated router (che può essere controllata tramite un parametro di priorità).

15.2.6 Gateway verso altri mondi

Nell'architettura di rete DNA è anche presente il concetto di gateway verso un'altra architettura di rete. In particolare, nelle reti DECnet è comune trovare gateway verso reti X.25 (ad esempio, in Italia Itapac) e verso reti IBM/SNA (figura 15.9).

I gateway sono collegati direttamente alla rete locale in modo che le loro funzionalità siano accessibili da tutti i nodi DECnet.

I gateway X.25 possono essere impiegati per vari scopi:

- come mezzi per definire dei DLM, cioè dei circuiti DECnet su X.25;
- come mezzi per fornire e/o utilizzare le reti X.25 in emulazione di terminale;
- come piattaforma di sviluppo di applicativi distribuiti basati su X.25 anche in ambiente multivendor non DECnet.

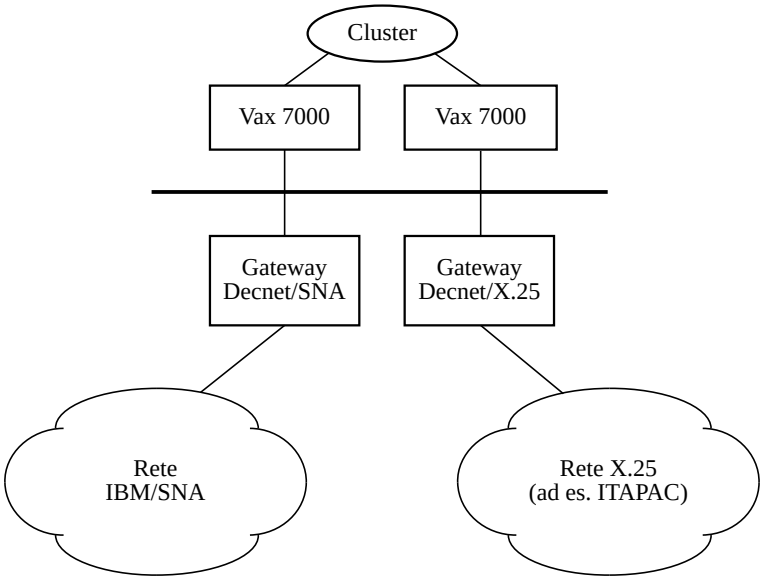


Fig. 15.9 - Gateway SNA e X.25.

I gateway DECnet/SNA permettono ai nodi di una rete DECnet di accedere ai principali applicativi di una rete IBM/SNA (ad esempio, emulazione 3270, remote job entry, accesso a basi di dati) e inoltre forniscono un ambiente per lo sviluppo di applicativi distribuiti, quali quelli basati su APPC/IBM (*Application Program to Program Communication*).

15.2.7 Cluster

La figura 15.9 illustra un esempio di cluster VAX formato da due VAX 7000. Il cluster è una modalità per interconnettere strettamente elaboratori omogenei con lo

scopo di far loro condividere lo stesso file system.

Dal punto di vista DECnet il cluster ha un indirizzo di rete per ogni nodo più, eventualmente, un indirizzo collettivo per tutto il cluster. Tale indirizzo collettivo viene gestito definendo i nodi che partecipano al cluster come L1.

Inoltre il bus CI può essere utilizzato anche come circuito DECnet. Normalmente esso viene definito ad un costo superiore a quello della LAN in modo da fungere da circuito di backup.

15.2.8 ATG

L'ATG (*Address Translation Gateway*) è una funzionalità di interconnessione di reti DECnet fase IV offerta da alcuni costruttori di router, tra cui Cisco.

Per comprendere tale funzionalità occorre ricordare che, essendo il routing di DECnet sempre e solo adattativo e dinamico, l'inserzione di un router tra due reti le trasforma automaticamente in una sola rete.

Questo molto spesso non è desiderato, per esempio se esistono problemi di sicurezza, e può portare a gravi malfunzionamenti se le due reti non hanno piani di indirizzamento compatibili.

L'ATG è una connessione più lasca in cui, tramite una tabella manuale scritta sul router che realizza l'ATG, si mappano pochi indirizzi di una rete su indirizzi dell'altra rete e viceversa [1]. Quindi le reti rimangono separate, ma alcuni calcolatori sono visibili su entrambe le reti. I loro indirizzi vengono modificati in modo da renderli compatibili con i due piani di indirizzamento che non devono essere modificati e restano tra loro incompatibili.

Ad esempio, un calcolatore con indirizzo 15.1 di una rete può essere reso visibile sull'altra rete con indirizzo 7.67.

15.3 ALTRI PROTOCOLLI DEC

Molti applicativi appartenenti alla DNA non utilizzano l'intera pila di protocolli DECnet in quanto appoggiano il protocollo applicativo direttamente sulla rete locale e quindi, non avendo il livello DRP, non possono essere instradati dai router.

Tali protocolli sono concepiti per essere limitati alla rete locale, eventualmente estesa con l'uso di bridge locali o remoti.

15.3.1 LAT e terminal server

Il LAT (*Local Area Transport*) è stato sviluppato per interconnettere in modo flessibile terminali e stampanti provvisti unicamente di interfacce seriali ad elaboratori tramite una LAN. Il collegamento avviene impiegando concentratori provvisti di una interfaccia LAN e più interfacce seriali, detti *terminal server* (figura 15.10), che si occupano di imbustare le trasmissioni seriali in pacchetti di rete locale. Per il collegamento di stampanti in rete esistono anche terminal server con interfaccia parallela.

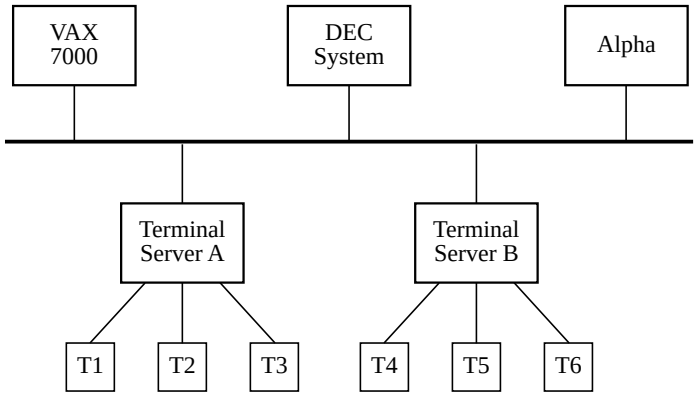


Fig. 15.10 - LAT e terminal server.

I terminal server utilizzano i protocolli LAT e telnet (paragrafo 16.12.1) per definire circuiti virtuali tra i terminali e i calcolatori. Ad esempio il terminal server A può avere attivi due circuiti virtuali, uno da T1 al VAX 7000 e l'altro da T3 al calcolatore Alpha, mentre il terminal server B può realizzarne altri tre: da T4 a VAX 7000, da T6 a VAX 7000 e da T5 a DEC System.

Un esempio di PDU LAT è riportato in appendice B, paragrafo B.5.

15.3.2 LAVC

Il LAVC (*Local Area VAX Cluster*) è un protocollo che permette ad elaboratori DEC di realizzare dei cluster, utilizzando come canale di comunicazione la rete locale invece del bus CI.

Questo protocollo si è diffuso rapidamente sugli elaboratori di fascia medio-bassa in quanto permette di ottenere la funzionalità di cluster senza dover effettuare

investimenti in hardware specializzato (molto spesso non disponibile).

Quando poi la rete locale utilizzata per il LAVC è separata da un bridge ed è o di tipo Ethernet con poche stazioni, o di tipo FDDI, allora anche le prestazioni sono competitive con la soluzione basata su CI.

15.3.3 MOP

Il MOP (*Maintenance Operation Protocol*) è utilizzato nell'architettura DNA per funzionalità di gestione della rete. Il MOP è stato concepito per il downline loading di software verso router, gateway e terminal server e per l'upline dumping della memoria di questi apparati in caso di malfunzionamento.

La modalità classica di operare di questo protocollo è la seguente: quando un router, un gateway o un terminal server viene acceso o reinizializzato, esso invia in multicast sulla LAN una richiesta di *memory load with transfer address*, cioè la richiesta di software da eseguire (detto nel seguito "immagine").

Alcuni nodi DECnet appartenenti alla LAN vengono abilitati a servire le richieste di MOP specificando anche quale immagine trasmettere, in funzione dell'indirizzo MAC del richiedente. Ad esempio, in figura 15.11 è mostrata una LAN su cui sono stati abilitati due nodi (per ragioni di affidabilità) a servire le richieste di MOP.

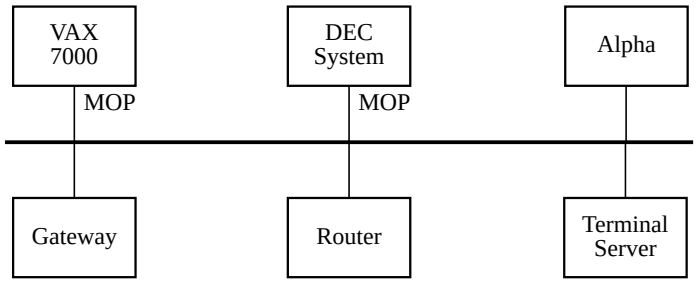


Fig. 15.11 - MOP.

I nodi abilitati rispondono alla richiesta ed inviano l'immagine. Il richiedente la carica in memoria e ne inizia l'esecuzione.

L'immagine caricata, una volta in esecuzione, può richiedere, sempre tramite il MOP, l'invio di altri programi eseguibili e/o di file di parametri oppure di effettuare il dump della memoria.

Un esempio di PDU MOP è riportato in appendice B, paragrafo B.7.2.

15.4 DECNET FASE V

Con DECnet fase V la DEC ha abbandonato i protocolli proprietari e ha costruito una piattaforma comprendente i livelli 1, 2 e 3 del modello di riferimento OSI, in modo assolutamente conforme a tale standard. Su tale piattaforma (figura 15.12) si appoggiano due pile di protocollo, quella OSI e quella DECnet fase IV.

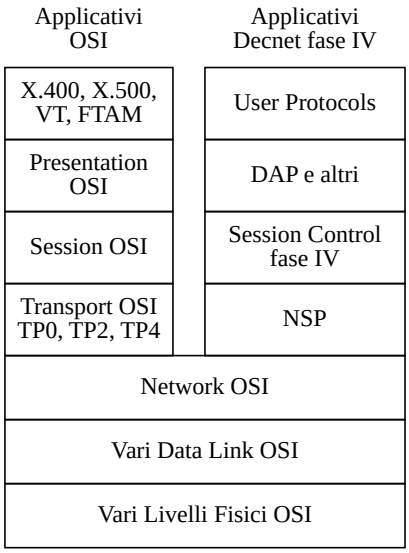


Fig. 15.12 - DECnet fase V.

Ai livelli 1 e 2 viene sostituito Ethernet con IEEE 802.3 e il DDCMP con HDLC, ma il cambiamento più importante avviene a livello 3 dove vengono adottati i protocolli OSI ed in particolare la scelta preferenziale è per il protocollo non connesso ISO 8473, per l'ES-IS ISO 9542 e per l'IS-IS ISO 10589.

In appendice B è mostrato un pacchetto generato dalla pila OSI di DECnet fase V e trasportato su un protocollo di livello 3 ISO 8473 (paragrafo B.6.1) e un pacchetto ISH (Intermediate System Hello) appartenente al protocollo ES-IS ISO 9542 (paragrafo B.6.3).

Con l'ISO 8473 vengono anche introdotti i nuovi indirizzi detti NSAP (Network Service Access Point) molto più ampi dei precedenti e univoci a livello mondiale.

Con ISO 10589 viene introdotto un algoritmo per il calcolo delle tabelle di instradamento di tipo LSP (Link State Packet) in luogo del distance vector di DECnet fase IV.

Con DECnet fase V viene introdotta una netta distinzione tra ES (*End System*) e IS (*Intermediate System*). Gli ES sono i calcolatori collegati ad una LAN, eventualmente con più di un collegamento (*multi-link* ES), senza per questo diventare router. Gli IS, cioè i router, sono realizzati da hardware dedicato.

Per facilitare la migrazione da fase IV a fase V viene garantito un certo livello di convivenza tra le due fasi. In particolare, a livello di LAN, nodi fase IV e fase V possono convivere (anche se i nodi fase IV non possono in questo modo trarre giovamento dal nuovo indirizzamento esteso) e aree DECnet diverse possono essere in fasi diverse (attenzione: tutti i router di un'area devono essere nella stessa fase).

Con DECnet fase V viene anche introdotto il DNS (*Domain Name Server*), cioè una base di dati distribuita che mantiene la corrispondenza tra nomi e indirizzi in modo consistente su tutta la rete.

Poiché DECnet fase V è totalmente conforme agli standard OSI, per una sua più approfondita discussione si rimanda al capitolo 17.

BIBLIOGRAFIA

[1] Cisco Systems, "Internetworking Technology Overview", Codice documento DOC-ITO13 78-1070-01, 1993.

[2] J. Martin, J. Leben, "DECnet Phase V: An OSI Implementation", Digital Press, Bedford MA (USA), 1992.

[3] Digital, "Digital's Networks: An Architecture With A Future", Documento Digital EB- 26013-42, 1984.

[4] Digital, "DECnet for OpenVMS Guide to Networking", Documento Digital AA-PV5ZA-TK, May 1993.

[5] ISO 8473, "Protocol for Providing the Connectionless-mode Network Service".

[6] ISO 9542, "End system to Intermediate system routeing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service".

[7] ISO 10589, "Intermediate system to Intermediate system Intra-Domain routeing information exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service".

16

L'ARCHITETTURA DI RETE TCP/IP

16.1 INTRODUZIONE

Nella prima metà degli anni '70, la Defence Advanced Research Project Agency (DARPA) dimostrò interesse per lo sviluppo di una rete a commutazione di pacchetto per l'interconnessione di calcolatori eterogenei, da utilizzarsi come mezzo di comunicazione tra le istituzioni di ricerca degli Stati Uniti. DARPA finanziò a tal scopo l'Università di Stanford e la BBN (Bolt, Beranek and Newman) affinché sviluppassero un insieme di protocolli di comunicazione.

Verso la fine degli anni '70, tale sforzo portò al completamento dell'*Internet Protocol Suite*, di cui i due protocolli più noti sono il TCP (*Transmission Control Protocol*) e l'IP (*Internet Protocol*).

Questi protocolli furono utilizzati da un gruppo di ricercatori per la rete ARPAnet e ottennero un elevato successo, anche perché posti sin dall'inizio nel dominio pubblico e quindi utilizzabili gratuitamente da tutti.

Il nome più accurato per l'architettura di rete rimane quello di Internet Protocol Suite, anche se comunemente si fa riferimento ad essa con la sigla TCP/IP o IP/TCP. Questo può portare ad alcune ambiguità: ad esempio è comune sentir parlare di NFS come un servizio basato su TCP/IP, anche se NFS non usa il protocollo TCP, ma un protocollo alternativo detto UDP appartenete all'Internet Protocol Suite. Visto l'uso estremamente comune della sigla TCP/IP, essa verrà adottata anche in questo libro in luogo del termine più corretto, quando non crei confusione.

TCP/IP è l'architettura adottata dalla rete Internet che, con le sue decine di milioni di calcolatori e il suo tasso di crescita del 5% al mese, è la più grande rete di calcolatori al mondo.

I protocolli appartenenti a questa architettura sono specificati tramite standard che si chiamano RFC (*Request For Comments*) facilmente reperibili sulla rete Internet. Famoso

è lo RFC 791 Internet Protocol, datato 1981, che specifica appunto il protocollo IP.

L'architettura TCP/IP ha dei componenti, quali l'IP, indubbiamente datati, ma non obsoleti: il grande successo di TCP/IP è quotidiano. Negli anni 1990, gli anni della maturità dell'ISO/OSI, l'unica architettura di rete che sembra interessare il mercato è quasi paradossalmente TCP/IP.

Anche gli enti di standardizzazione nazionali e internazionali hanno dovuto arrendersi davanti alla massiccia diffusione di TCP/IP e dargli la stessa dignità di ISO/OSI.

16.2 ARCHITETTURA

La figura 16.1 mostra l'architettura dell'Internet Protocol Suite e la paragona con il modello di riferimento ISO/OSI. Questa architettura permette l'esistenza di più pile di protocolli alternative tra loro ed ottimizzate per determinate applicazioni.

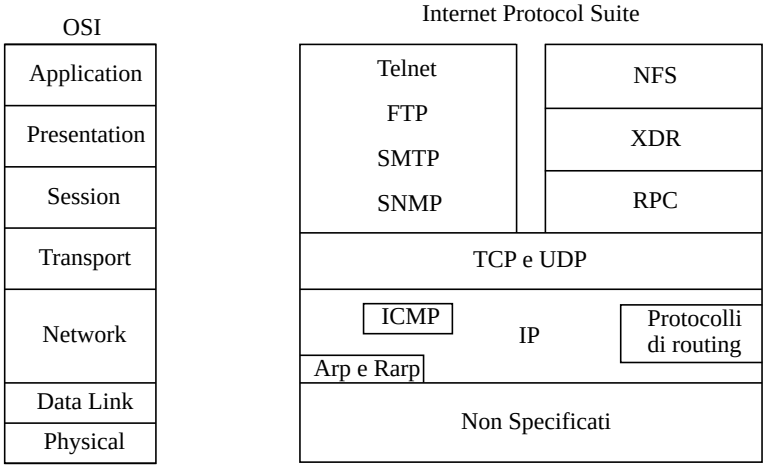


Fig. 16.1 - Internet Protocol Suite.

Esempi di possibili pile sono: telnet/TCP/IP/Ethernet, FTP/TCP/IP/Ethernet, SNMP/UDP/IP/FDDI e NFS/XDR/RPC/UDP/IP/Token-Ring.

16.3 SOTTO L'IP

L'architettura di rete TCP/IP non specifica i livelli 1 e 2 della rete, ma utilizza quelli normalmente disponibili e conformi agli standard. Ad esempio, nell'ambito

delle reti locali opera su Ethernet/IEEE802.3, Token-Ring e FDDI; nell'ambito delle reti geografiche su HDLC, PPP, SLIP, X.25, Frame Relay, SMDS e ATM.

Esistono anche realizzazioni per reti molto strane, spesso diffuse solo all'interno di certe comunità, ad esempio AIX.25, una rete packet switched dei radioamatori.

16.4 IL PROTOCOLLO IP

Il protocollo IP (*Internet Protocol*) è il protocollo principale del livello 3 (Network) dell'architettura TCP/IP. Si tratta di un protocollo semplice, di tipo datagram, non connesso (connectionless o CLNS), specificato in RFC 791. Insieme a TCP costituisce il nucleo originale e principale dell'Internet Protocol Suite.

IP si occupa di instradare i messaggi sulla rete, ma ha anche funzioni di frammentazione e riassemblaggio dei messaggi e di rilevazione (non correzione) degli errori.

Il formato dell'header del pacchetto IP è mostrato in figura 16.2. Esempi di pacchetti IP sono riportati in appendice B, paragrafo B.3.

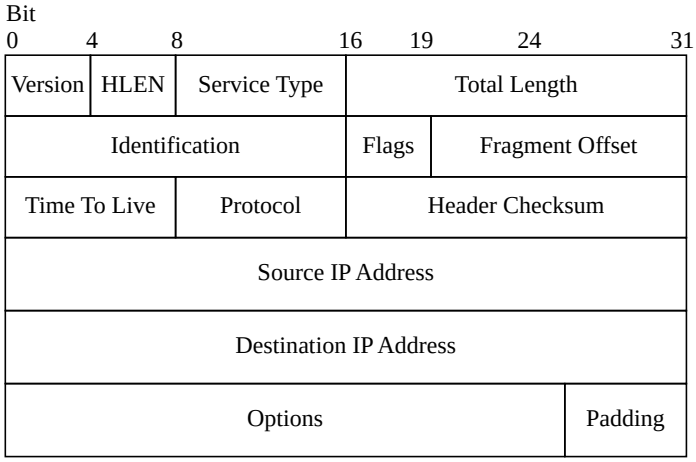


Fig. 16.2 - Header del pacchetto IP.

Il significato dei campi del pacchetto IP è il seguente:

- *Version*: è il numero di versione del protocollo IP che ha generato il pacchetto; attualmente questo campo vale sempre 4;
- *HLEN (Header LENgth)*: è la lunghezza dell'header IP, variabile in funzione del campo option, espressa come numero di parole da 32 bit;

- *service type*: specifica come un protocollo di livello superiore vuole che il pacchetto sia trattato; è possibile assegnare vari livelli di priorità utilizzando questo campo;
- *total length*: è la lunghezza del pacchetto IP (header più dati) in byte;
- *identification*: questo campo contiene un numero intero che identifica il pacchetto; è usato per permettere il riassemblaggio di un pacchetto frammentato;
- *flags*: specificano se un pacchetto può essere frammentato e se si tratta dell'ultimo frammento di un pacchetto;
- *fragment offset*: è l'offset del frammento in multipli di 8 byte;
- *time to live*: è un contatore che viene decrementato con il passaggio del tempo; quando il contatore arriva a zero il pacchetto viene scartato. Permette di eliminare i pacchetti che, a causa di un malfunzionamento, sono entrati in loop;
- *protocol*: identifica il protocollo di livello superiore contenuto nel campo dati del pacchetto. In appendice A, paragrafo A.7, sono riportati i codici dei protocolli che possono essere contenuti nel campo dati di IP;
- *header checksum*: è un campo utilizzato per controllare che l'header IP sia corretto;
- *source e destination address*: sono gli indirizzi IP di mittente e destinatario, entrambi su 32 bit;
- *option*: è un campo usato dall'IP per fornire varie opzioni, quali la sicurezza e il source routing, che può essere di tipo loose o strict.

L'header IP è seguito dal campo dati che contiene la PDU del protocollo di livello superiore.

16.5 INDIRIZZAMENTO IP

L'indirizzamento IP è parte integrante del processo di instradamento dei messaggi sulla rete. Gli indirizzi IP, che devono essere univoci sulla rete, sono lunghi 32 bit (quattro byte) e sono espressi scrivendo i valori decimali di ciascun byte separati dal carattere punto.

Esempi di indirizzi IP sono: `34.0.0.1`, `129.130.7.4` e `197.67.12.3`.

Agli indirizzi IP si associano per comodità uno o più nomi che possono essere definiti localmente in un file "hosts" che ha il seguente formato:

```
223.1.2.1  alpha
223.1.2.2  beta
223.1.2.3  gamma
223.1.2.4  delta    mycomputer
223.1.3.2  epsilon
223.1.4.2  iota
```

Questo approccio diviene impraticabile quando la rete IP cresce di dimensione e allora si preferisce utilizzare una base di dati distribuita per la gestione dei nomi (si veda il paragrafo 16.12.4).

Gli indirizzi IP comprendono due o tre parti. La prima parte indica l'indirizzo della rete (network), la seconda (se presente) quello della sottorete (subnet) e la terza quello dell'host.

Occorre subito evidenziare che non sono i nodi ad avere un indirizzo IP, bensì le interfacce. Quindi se un nodo ha tre interfacce, esso ha tre indirizzi IP. Poiché la maggior parte dei nodi ha una sola interfaccia, è comune parlare dell'indirizzo IP di un nodo. Questo tuttavia è senza dubbio sbagliato nel caso dei router che hanno, per definizione, più di una interfaccia.

Gli indirizzi IP sono assegnati da un'unica autorità e quindi sono garantiti univoci a livello mondiale*. Essi vengono assegnati a gruppi come dettagliato nel seguito.

Gli indirizzi IP sono suddivisi in cinque classi, come schematizzato in figura 16.3.

- Classe A. Sono concepiti per poche reti di dimensioni molto grandi. I bit che indicano la rete sono 7 e quelli che indicano l'host 24. Quindi si possono avere al massimo 128 reti di classe A, ciascuna con una dimensione massima di circa 16 milioni di indirizzi. Gli indirizzi di classe A sono riconoscibili in quanto il primo campo dell'indirizzo è compreso tra 0 e 127.
- Classe B. Sono concepiti per un numero medio reti di dimensioni medio-grandi. I bit che indicano la rete sono 14 e quelli che indicano l'host 16. Quindi si possono avere al massimo circa 16000 reti di classe B, ciascuna con una dimensione massima di circa 64000 indirizzi. Gli indirizzi di classe B sono riconoscibili in quanto il primo campo dell'indirizzo è compreso tra 128 e 191.
- Classe C. Sono concepiti per moltissime reti di dimensioni piccole. I bit che indicano la rete sono 21 e quelli che indicano l'host 8. Quindi si possono avere al massimo 2 milioni di reti di classe C, ciascuna con una dimensione massima di 256 indirizzi. Gli indirizzi di classe C sono riconoscibili in quanto il primo campo dell'indirizzo è compreso tra 192 e 223.

* In Italia esistono vari soggetti che possono assegnare indirizzi Internet. Chi fosse interessato può contattare, ad esempio, il GARR/NIS, c/o CNUCE/CNR, Via Santa Maria 36, 56126 Pisa, Tel. 050-593111, Fax 050-904052.

- Classe D. Sono riservati ad applicazioni di multicast secondo quanto descritto nel RFC 1112. In appendice A, paragrafo A.6, sono elencati gli indirizzi IP di multicast attualmente assegnati. Gli indirizzi di classe D sono riconoscibili in quanto il primo campo dell'indirizzo è compreso tra 224 e 239.
- Classe E. Questi indirizzi sono riservati per usi futuri. Gli indirizzi di classe E sono riconoscibili in quanto il primo campo dell'indirizzo è compreso tra 240 e 255.

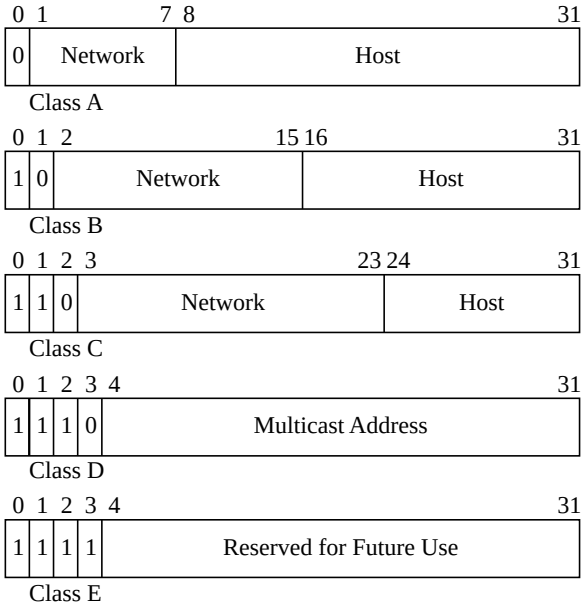


Fig. 16.3 - Classi di indirizzi.

In appendice A, paragrafo A.5, sono riportati gli indirizzi IP con significato particolare, ad esempio broadcast e loopback.

La parte host di un indiririzzo di classe A, B o C può essere ulteriormente divisa in due parti: la subnet e l'host. La figura 16.4 mostra un indirizzo di classe B prima e dopo il subnetting. Il subnetting è discusso nel RFC 950.

L'ampiezza dei campi subnet e host può essere definita in modo molto flessibile tramite un parametro detto *netmask*. La netmask contiene bit a uno in corrispondenza dei campi network e subnet, e a zero in corrispondenza del campo host.

Ad esempio una netmask 11111111111111111111111100000000, più comunemente scritta come indirizzo IP 255.255.255.0 o in esadecimale ffffff00, indica che il campo host coincide con l'ultimo byte dell'indirizzo.

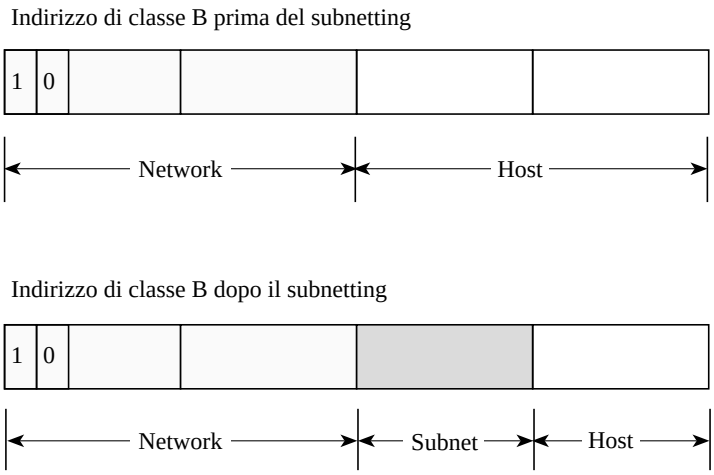


Fig. 16.4 - Subnetting.

All'interno di una network IP la netmask deve essere univoca, in quanto il partizionamento della network in subnet deve essere univoco. La netmask viene messa in AND bit a bit con gli indirizzi IP per estrarre la parte network e subnet. Tramite questo procedimento è possibile verificare se due indirizzi appartengono alla stessa subnet.

Ad esempio si supponga di aver una netmask 255.255.254.0 e i due indirizzi 128.155.4.77 e 128.155.5.75. Mettendo in AND bit a bit gli indirizzi con la netmask si ottiene in entrambi i casi 128.155.4.0 e quindi gli indirizzi appartengono alla stessa subnet. Un caso di due indirizzi simili ai precedenti, ma appartenti a subnet diverse è 128.155.5.75 e 128.155.6.77, in quanto i due AND rendono rispettivamente i valori 128.155.4.0 e 128.155.6.0.

L'importanza di comprendere se due indirizzi appartengono o no alla stessa subnet è fondamentale in quanto il primo livello di routing è implicito nella corrispondenza fissata in TCP/IP tra reti fisiche e subnet: *una rete fisica deve coincidere con una subnet IP*.

Questa situazione è illustrata in figura 16.5 dove sono mostrate più reti fisiche e le subnet IP associate. La rete è di classe A (primo byte uguale a 11) e ha una netmask 255.255.0.0.

Nell'esempio sono presenti le subnet 11.1 e 11.2. Si noti che il bridge, operando a livello 2 ed essendo trasparente al protocollo IP, collega reti Ethernet appartenenti alla stessa subnet 11.1, mentre il router collega reti Ethernet appartenenti a subnet diverse (11.1 e 11.2). A tal scopo il router ha due indirizzi IP diversi: uno appartenente alla subnet 11.2 (11.2.0.254) e uno appartenente alla subnet 11.1 (11.1.0.253).

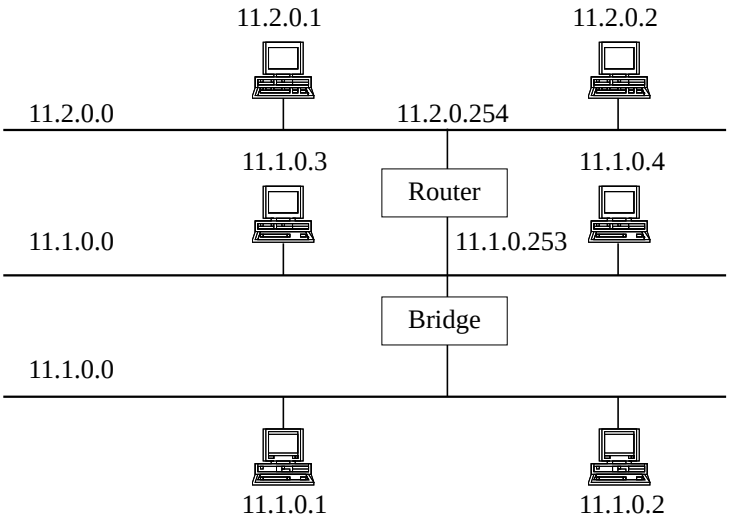


Fig. 16.5 - Indirizzi e reti fisiche.

Il bridge, essendo trasparente ai protocolli di livello superiore, non ha indirizzi IP.

La regola che impone una corrispondenza biunivoca tra subnet IP e reti fisiche è stata ultimamente leggermente rilassata per le LAN, dove è ammesso dalle implementazioni più recenti di TCP/IP che ad una LAN possano essere associate più subnet IP. Continua a non valere il viceversa.

Il concetto di subnet introduce un livello di gerarchia nelle reti TCP/IP. Il routing diventa un routing all'interno della subnet e tra subnet.

Il routing all'interno della subnet è banale in quanto la subnet coincide con una rete fisica che garantisce la raggiungibilità diretta delle stazioni ad essa collegate. L'unico problema che si può incontrare è quello di mappare gli indirizzi IP nei corrispondenti indirizzi di livello 2. Questo mappaggio è oggi quasi sempre gestito in modo automatico, tramite i protocolli ARP e RARP descritti nel seguito.

Il routing tra le subnet è gestito dagli IP router che originariamente erano stati definiti gateway. Tale definizione è infelice in quanto gli IP gateway sono quelli che OSI chiama router e i gateway OSI non hanno un corrispettivo nel mondo TCP/IP.

Nel seguito del capitolo si useranno i termini IP router e gateway come sinonimi.

Gli IP router effettuano l'instradamento sulla base di tabelle di instradamento che possono essere scritte manualmente dal gestore della rete o calcolate automaticamente tramite una serie di algoritmi di tipo distance vector o link state packet, descritti nel paragrafo 16.9.

Per comprendere meglio i concetti esposti sino a questo punto si consideri l'esempio di figura 16.6.

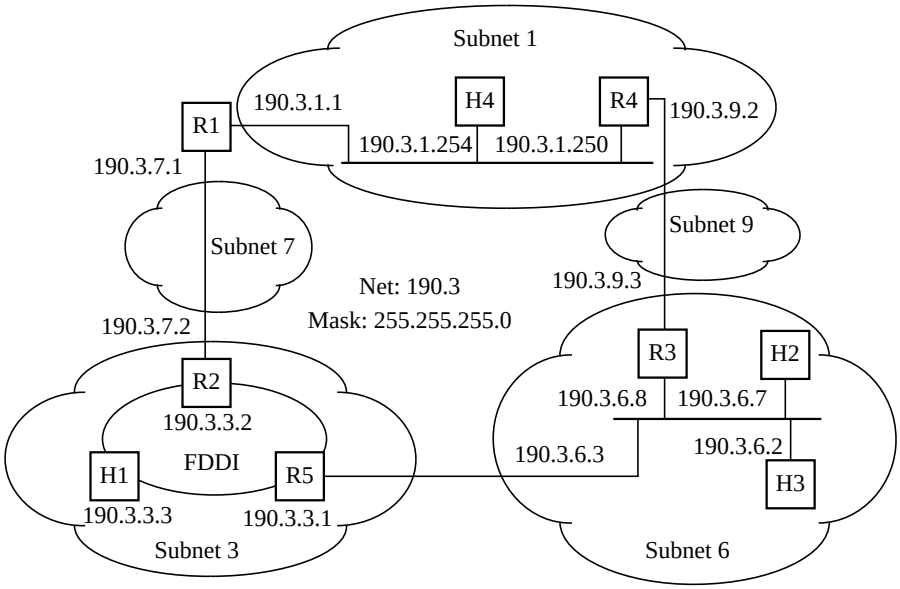


Fig. 16.6 - Esempio di indirizzamento IP.

In tale esempio la network 190.3 di classe B è stata partizionata in 256 subnet, grandi ciascuna 256 indirizzi. Nell'esempio sono utilizzate 5 subnet: la 190.3.1.0, la 190.3.3.0, la 190.3.6.0, la 190.3.7.0 e la 190.3.9.0.

Di queste cinque subnet, due corrispondono a reti fisiche di tipo Ethernet (la 190.3.6.0 e la 190.3.1.0), una ad una rete FDDI (la 190.3.3.0) e due a canali geografici di tipo punto-punto (la 190.3.7.0 e la 190.3.9.0).

Si noti che nel modello di gerarchia TCP/IP i router non fanno parte delle subnet, ma sono ad esse esterni. Inoltre non esiste il concetto di collegare direttamente due router: il collegamento avviene sempre tramite una subnet, eventualmente di tipo punto-punto e quindi formata da due soli indirizzi.

I router hanno tanti indirizzi quante sono le interfacce e quindi le subnet che collegano. Ad esempio il router R5 ha due indirizzi, uno associato alla rete FDDI (190.3.3.1) e l'altro associato alla rete Ethernet (190.3.6.3).

Sempre considerando il router R5, esso deve avere una tabella di instradamento che comprenda una entry per tutte le subnet cui il router non è direttamente collegato (in questo caso tre: la 190.3.1.0, la 190.3.7.0 e la 190.3.9.0).

La tabella di instradamento può essere simile a quella riportata in tabella 16.1.

Subnet di destinazione	Indirizzo del router cui inviare il pacchetto
190.3.1.0	190.3.3.2
190.3.7.0	190.3.3.2
190.3.9.0	190.3.6.8

Tab. 16.1 - Esempio di tabella di instradamento.

Si noti come tutti gli indirizzi della seconda colonna debbano appartenere a reti cui il router è direttamente connesso: nell'esempio appartengono infatti alle subnet 3 e 6 cui R5 è connesso.

La tabella di instradamento può essere creata manualmente con comandi del tipo:

```
route add 190.3.1.0 190.3.3.2
route add 190.3.7.0 190.3.3.2
route add 190.3.9.0 190.3.6.8
```

oppure calcolata dagli appositi algoritmi di routing descritti nel paragrafo 16.9.

Si noti che occorre anche definire per ogni host quale sia il suo router di default. Ad esempio, per l'host H4 si può definire che il router di default è R1, con un comando del tipo:

```
route add default 190.3.1.1
```

dato sul nodo H4 stesso.

Quando il nodo H4 deve trasmettere un pacchetto, per prima cosa verifica se il pacchetto è destinato ad un nodo appartenente alla sua stessa subnet. Se questo è il caso, la trasmissione può avvenire direttamente. In caso contrario invia il pacchetto al router di default (in questo caso R1). R1 instrada il messaggio a destinazione. Se durante tale operazione di instradamento R1 si trova a ritrasmettere il messaggio sulla stessa rete da cui lo ha ricevuto, ad esempio perché il messaggio è destinato alla subnet 9 e lo invia a R4, allora invia anche un messaggio di routing redirect al nodo mittente, in questo caso H4.

Il messaggio di routing redirect è inviato usando il protocollo ICMP che si appoggia su IP (si veda paragrafo 16.6).

Quando H4 ha deciso a quale indirizzo IP inviare il messaggio deve scoprire, se già non lo sa, qual è l'indirizzo di livello 2 (nel caso delle LAN l'indirizzo MAC) del destinatario. Per fare ciò utilizza il protocollo ARP descritto nel paragrafo 16.7.

16.6 IL PROTOCOLLO ICMP

Il protocollo Internet Control Message Protocol (ICMP) è stato progettato per riportare anomalie che accadono nel routing di pacchetti IP e verificare lo stato della rete. ICMP è specificato nel RFC 792.

La tabella 16.2 riporta i tipi di pacchetti ICMP.

Type Field	Message Type
0	Echo Reply
3	Destination Unreachable
4	Source Quence
5	Redirect
8	Echo Request
11	Time Exceeded for a Datagram
12	Parameter Problem on a Datagram
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

Tab. 16.2 - Tipi di Messaggi ICMP.

I messaggi che riportano anomalie sono, ad esempio, *destination unreachable, time exceeded for a datagram* e *parameter problem on a datagram.*

I messaggi di verifica della raggiungibilità di un nodo sono *echo request* e *echo reply*.

Il messaggio *redirect* indica una condizione di stimolo ad un routing migliore, in quanto un router è stato attraversato inutilmente (ha dovuto ritrasmettere il messaggio sulla stessa rete da cui lo ha ricevuto).

Quando un host riceve un pacchetto di routing redirect tratta l'informazione in esso contenuta in modo simile a quella specificata da un comando di route add ed associa quindi un router diverso da quello di default a quella destinazione.

Gli ultimi messaggi ad essere stati introdotti nel protocollo ICMP sono *address mask request* e *address mask reply*, per permettere ad una interfaccia di scoprire automaticamente la netmask usata in quella network.

16.7 I PROTOCOLLI ARP E RARP

I protocolli *Address Resolution Protocol* (ARP) e *Reverse Address Resolution Protocol* (RARP) sono utilizzati per scoprire in modo automatico le corrispondenze tra gli indirizzi di livello 3 e gli indirizzi di livello 2 e viceversa. Questo è importante nelle LAN dove occorre creare una relazione tra gli indirizzi IP e gli indirizzi MAC.

I protocolli ARP e RARP sono specificati nel RFC 826.

Il protocollo ARP viene usato tutte le volte che una stazione collegata ad una LAN deve inviare un messaggio ad un nodo sulla stessa LAN di cui conosce unicamente l'indirizzo di livello 3.

Il protocollo RARP viene invece utilizzato dalle stazioni non dotate di memoria di massa (diskless) per scoprire il loro indirizzo IP in fase di bootstrap.

La figura 16.7 mostra la PDU di ARP/RARP.

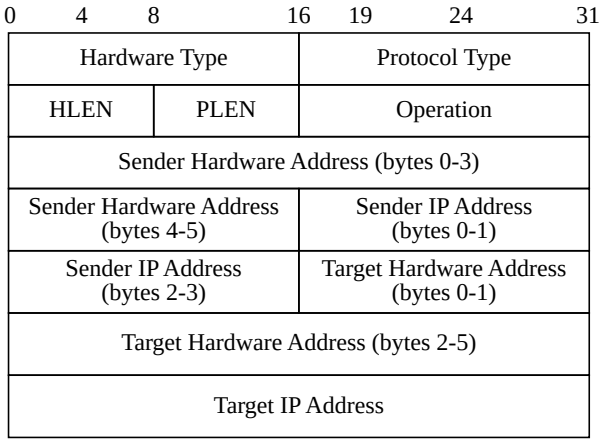


Fig. 16.7 - Il pacchetto ARP.

I protocolli ARP e RARP si appoggiano direttamente sulle reti locali e non su IP, come invece avviene nel caso di ICMP. Essi operano inviando le loro richieste in broadcast a tutte le stazioni della rete, anche quelle che non utilizzano TCP/IP.

La richiesta in broadcast di ARP contiene l'indirizzo IP del nodo di cui si vuole scoprire l'indirizzo di livello 2. Il nodo avente l'indirizzo IP specificato risponde alla richiesta fornendo il suo indirizzo di livello 2. Il protocollo RARP funziona in modo simile, ma è fornito un indirizzo di livello 2 e richiesto un indirizzo IP.

L'appendice A, paragrafo A.9, riporta i vari parametri del protocollo ARP, mentre un esempio di PDU ARP è riportata in appendice B, paragrafo B.3.3.

Per aumentare l'efficienza, i nodi mantengono in una cache locale le risposte ricevute alle richieste di ARP. Ad esempio, in figura 16.8 è mostrato il formato di ogni singola entry della ARP cache, come realizzata nel software Microsoft TCP/IP.

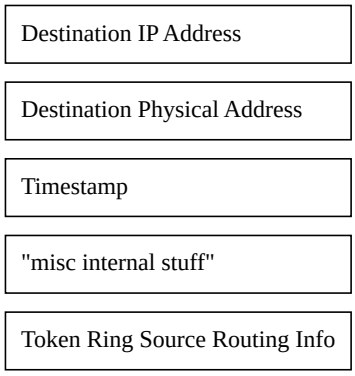


Fig. 16.8 - Una entry nella cache di ARP.

Il campo *timestamp* serve ad eliminare dalla cache le entry che sono più vecchie di 15 minuti.

Il contenuto della cache di ARP può essere visualizzato, in molte realizzazioni, tramite il comando:

```
arp -a
```

16.8 GLI AUTONOMOUS SYSTEM

Sino a questo punto il routing di TCP/IP è stato descritto come gerarchico su due livelli: un primo livello all'interno della subnet, implicito in quanto gestito dalla rete fisica; un secondo livello tra subnet gestito dagli IP router tramite tabelle di instradamento. Le subnet derivano dalla suddivisione di una network.

Le network sono ulteriormente raggruppate in *Autonomous System (AS)*, cioè in gruppi di network controllate e gestite da un'unica autorità.

Gli autonomus system sono identificati da un numero intero, univoco a livello mondiale, assegnato dalla stessa autorità che rilascia gli indirizzi Internet.

I router che instradano i messaggi all'interno dello stesso AS sono detti *interior router*, mentre quelli che instradano i messaggi anche tra AS diversi sono detti *exterior router*.

Un esempio di interconnessione di due AS è mostrato in figura 16.9.

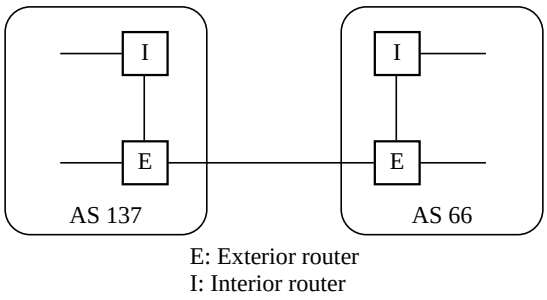


Fig. 16.9 - Exterior ed interior router.

Gli interior router possono scambiare informazioni di instradamento tramite un IGP (*Interior Gateway Protocol*), mentre gli exterior router utilizzano un EGP (*Exterior Gateway Protocol*).

Nei sottoparagrafi seguenti vengono illustrati i principali protocolli di routing di tipo EGP e IGP.

All'interno di un AS normalmente si usa lo stesso IGP su tutti i router.

16.9 I PROTOCOLLI DI ROUTING

L'architettura TCP/IP ha una varietà di protocolli di routing addirittura eccessiva. Nel seguito verranno discussi solo quelli che hanno maggior rilievo nella realtà italiana.

16.9.1 RIP

Il *Routing Information Protocol* (RIP) è un IGP originariamente progettato dalla Xerox per la sua rete XNS. È stato introdotto nell'architettura TCP/IP dall'Università di Berkeley nel 1982, definito come RFC 1058 nel 1988 e aggiornato con il RFC 1388 nel 1993.

RIP ha avuto una grandissima diffusione, soprattutto nelle implementazioni di reti di personal computer, ed è alla base di molti altri protocolli di routing: Novell, 3Com, Banyan, ecc.

RIP è un protocollo di tipo distance vector in cui ogni router invia il suo distance vector ai router adiacenti, ogni 30 secondi (si veda paragrafo 14.6). Le tabelle di instradamento memorizzano un solo cammino per ogni destinazione.

Il limite principale di RIP è che permette un numero massimo di hop pari a 15: ogni

destinazione più lontana di 15 hop viene considerata non raggiungibile.

Inoltre RIP ignora le velocità delle linee, non permette di definire costi o altre metriche, ma basa l'instradamento solo sulla minimizzazione del numero di hop. In caso di modifiche della topologia della rete, RIP è lento a convergere.

Per queste ragioni RIP può essere utilizzato solo in reti di piccole dimensioni.

Un esempio di PDU RIP è riportata in appendice B, paragrafo B.3.9.

16.9.2 IGRP

L'*Interior Gateway Routing Protocol* (IGRP) è un IGP sviluppato da Cisco System Inc. a metà degli anni 1980 per superare i limiti di RIP [5,6].

Si tratta anche in questo caso di un protocollo di tipo distance vector, ma con una metrica molto sofisticata. La scelta del cammino migliore è effettuata da IGRP combinando dei vettori di metriche contenenti: ritardo, banda, affidabilità, lunghezza massima del pacchetto e carico.

Inoltre IGRP permette il *multipath routing*, cioè la suddivisione del traffico tra più linee parallele. Il carico viene suddiviso in funzione delle metriche associate alle linee.

IGRP è nato come protocollo proprietario Cisco e sinora è stato reso disponibile solo sui router Cisco. A questo limite principale occorre aggiungere quelli generali, meno importanti, degli algoritmi distance vector descritti nel paragrafo 14.6.

16.9.3 OSPF

L'*Open Shortest Path First* (OSPF) è un IGP sviluppato appositamente per TCP/IP dall'IETF (*Internet Engineering Task Force*). Il gruppo di lavoro è stato costituito nel 1988 con lo scopo di realizzare un protocollo di tipo *link state packet* (si veda paragrafo 14.7) per TCP/IP.

OSPF è stato definito dal RFC 1247 nel 1991 e ridefinito dal RFC 1583 nel 1994.

OSPF ha il concetto di gerarchia. La radice della gerarchia è l'AS che può essere suddiviso in aree, ciascuna delle quali contiene un gruppo di reti contigue.

Il routing all'interno di un'area è detto intra-area, quello tra aree diverse inter-area. Ogni AS ha un'area detta di *backbone* ed identificata con 0.0.0.0 o più semplicemente 0. La backbone area (detta più semplicemente nel seguito backbone) può essere anche non contigua; in tal caso occorre configurare dei *virtual links* per garantire la coesione del backbone.

I router OSPF sono classificati secondo quattro categorie non mutuamente

esclusive:

- *Internal router*. Un router in cui tutte le network direttamente connesse appartengono alla stessa area. Questi router utilizzano una sola copia dell'algoritmo OSPF. I router che hanno solo interfacce sul backbone appartengono a questa categoria.
- *Area border router*. Un router che collega più aree. Questi router utilizzano più copie dell'algoritmo OSPF: una copia per ogni area direttamente connessa e una copia per il backbone. Gli area border router condensano le informazioni delle aree a loro collegate e le ridistribuiscono sul backbone. Il backbone ridistribuisce a sua volta queste informazioni alle altre aree.
- *Backbone router*. Un router che ha una interfaccia sul backbone. Questo include tutti i router che si collegano a più di un'area (area border router). I backbone router che hanno tutte le interfacce sul backbone sono considerati internal router.
- *AS boundary router*. Un router che scambia informazioni di routing con altri router appartenenti ad altri AS. Questa classificazione è ortogonale alle altre precedenti: un AS boundary router può essere un internal o area border router.

La figura 16.10 mostra un esempio di AS TCP/IP suddiviso in tre aree OSPF e connesso ad un altro AS.

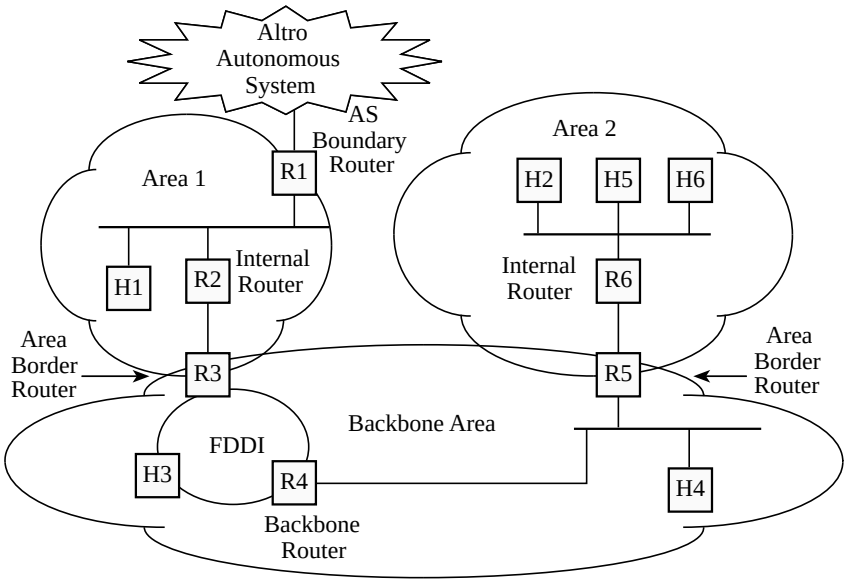


Fig. 16.10 - Esempio di utilizzo di OSPF.

OSPF è il protocollo più promettente per il routing di TCP/IP. Esso è infatti disponibile sui router di tutti i costruttori, è in grado di gestire reti di grosse dimensioni ed utilizza la tecnologia *Link State Packet* (LSP, paragrafo 14.7), che rappresenta lo stato dell'arte.

16.9.4 Integrated IS-IS

L'*integrated IS-IS*, detto anche *dual IS-IS*, è una versione del protocollo IS-IS (ISO 10589) che è in grado di ospitare informazioni di routing anche per protocolli diversi dall'OSI CLNS (ISO 8473). Per una discussione sui protocolli OSI si veda il capitolo 17.

Nell'ambito di un router multiprotocollo, questo approccio alla gestione di un solo protocollo di routing, comune a tutte le architetture di rete, si contrappone a quello più classico di avere un protocollo di routing per ogni architettura di rete e può portare ad una certa economia nell'utilizzo delle risorse di rete dei router.

16.9.5 EGP

L'Exterior Gateway Protocol è il primo EGP* ad essere stato ampiamente utilizzato all'interno della rete Internet. Specificato con RFC 904 nell'aprile 1984 è oggi ampiamente disponibile su tutti i router, anche se è ormai considerato un protocollo obsoleto e Internet lo sta sostituendo con il BGP (si veda il paragrafo 16.9.6).

EGP è simile ad un algoritmo distance vector, ma invece del concetto di costo specifica solo se la destinazione è raggiungibile oppure no. Questo ne impedisce il funzionamento su topologie magliate.

Esiste il concetto di un *core system* formato da una interconnessione di *core router* (figura 16.11).

EGP genera dei pacchetti di routing update che contengono informazioni di *network reachability*, cioè annunciano che certe reti sono raggiungibili attraverso certi router. I pacchetti di routing update sono inviati ai router vicini ad intervalli di tempo regolari e raggiungono tutti i router EGP. L'informazione in essi contenuta è utilizzata per costruire le tabelle di instradamento.

---

* Si noti che con il termine EGP si indica sia un generico protocollo di exterior routing, sia lo specifico protocollo oggetto del presente paragrafo.

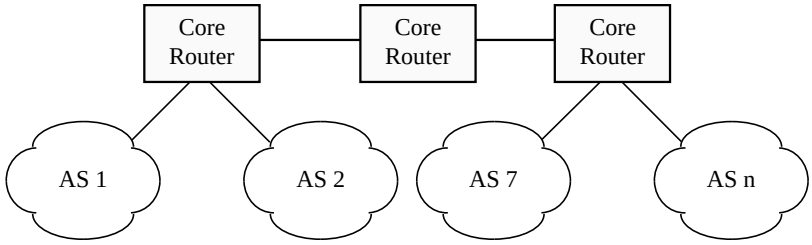


Fig. 16.11 - Esempio di utilizzo di EGP.

I limiti di EGP sono molti e gravi: EGP non ha una metrica associata alle linee e quindi basa le sue decisioni esclusivamente sulla raggiungibilità; EGP non ammette la presenza di magliature nella topologia, e tutti gli AS devono essere collegati in modo stellare ad un core system; i pacchetti di routing update possono essere molto grandi.

16.9.6 BGP

Il *Border Gateway Protocol* (BGP) è un exterior gateway protocol pensato per rimpiazzare il protocollo EGP ormai obsoleto. Il BGP è specificato per la prima volta dal RFC 1105 nel 1988, rispecificato come BGP-2 nel RFC 1163 nel 1990 e rispecificato ancora come BGP-3 nel RFC 1267 del 1991.

I router BGP comunicano tra loro utilizzando un livello di trasporto affidabile. Il BGP è un algoritmo di tipo distance vector, ma invece di trasmettere il costo di una destinazione, trasmette la sequenza di autonomous system da attraversare per raggiungere quella destinazione.

Ogni router calcola il suo instradamento preferito verso una data destinazione e lo comunica ai router BGP adiacenti tramite un distance vector. La politica con cui tale calcolo avviene è configurabile su ogni router BGP.

16.9.7 CIDR

Il *Classless Inter Domain Routing* (CIDR) è una modalità di propagazione dell'informazione di raggiungibilità (in gergo "annuncio") delle reti IP, che associa ad ogni indirizzo annunciato una netmask.

Il CIDR è specificato negli RFC 1517, 1518, 1519 e 1520.

Nei protocolli non CIDR la netmask viene derivata dalla classe dell'indirizzo. Con il CIDR questo non è vero ed indirizzi contigui possono essere propagati come fossero un indirizzo solo, operazione detta anche di clustering.

Ad esempio si supponga di volere annunciare le quattro seguenti reti di classe C: 199.9.4.0, 199.9.5.0, 199.9.6.0 e 199.9.7.0. Esse possono essere annuncate contemporaneamente tramite l'indirizzo 199.9.4.0 e la netmask 255.255.252.0.

Il CIDR riduce notevolmente la quantità di informazioni che devono essere propagate dagli EGP e anche dagli IGP e quindi ne aumenta l'efficienza. OSPF, Integrated IS-IS e la versione 4 del BGP realizzano il CIDR.

16.10 IL PROTOCOLLO TCP

Il TCP è un protocollo di transport di tipo connection-oriented che fornisce un servizio di tipo full-duplex (bidirezionale-contemporaneo), con acknowledge (conferma) e controllo di flusso.

Il TCP è utilizzato dalle applicazioni di rete che richiedono una trasmissione affidabile dell'informazione. Le applicazioni si connettono alle porte TCP e ad alcune applicazioni principali sono associate delle *well know port* cioè delle porte che hanno lo stesso numero su tutti i calcolatori (ad esempio all'applicazione telnet è associata la porta 23).

Il TCP segmenta e riassembla i dati secondo le sue necessità: ad esempio se un'applicazione fa cinque scritture su una porta TCP, l'applicazione destinataria può dover effettuare 10 letture per ottenere tutti i dati, oppure ottenerli tutti in una sola lettura.

Il TCP è un protocollo a sliding window (finestre) con meccanismi di time-out e ritrasmissione. La ricezione dei dati deve essere confermata dall'applicazione remota. La conferma può essere inserita in una PDU in transito nella direzione opposta, con una tecnica di piggybacking (si veda il paragrafo 13.2).

Come tutti i protocolli di tipo *sliding window*, TCP ha un massimo numero di dati in attesa di acknowledge. In TCP tale dimensione massima è specificata come numero di byte (window) e non come numero di segmenti TCP.

Il formato dell'header del pacchetto TCP è mostrato in figura 16.12, mentre un esempio di pacchetto TCP su IP è riportato in appendice B, paragrafo B.3.1.

I significati dei campi del pacchetto sono i seguenti:

- La *source port* e la *destination port* sono i numeri delle porte cui sono associati gli applicativi che usano la connessione TCP.

- Il *sequence number* è il numero di sequenza del primo byte del campo dati del messaggio. È utilizzato anche come identificatore della sliding window.
- Lo *acknowledge number* è il campo di acknowledge con tecnica di piggybacking della trasmissione nella direzione opposta. Contiene il numero di sequenza del primo byte che il mittente si aspetta di ricevere.
- Il campo *data offset* indica il numero di parole da 32 bit che compongono l'header TCP, variabile in funzione del campo option.
- Il campo *flag* contiene informazioni varie.
- Il campo *window* contiene la dimensione della receiving window del TCP mittente e quindi lo spazio disponibile nei buffer per il traffico entrante.
- Il campo *urgent pointer* punta al primo byte urgente nel pacchetto.

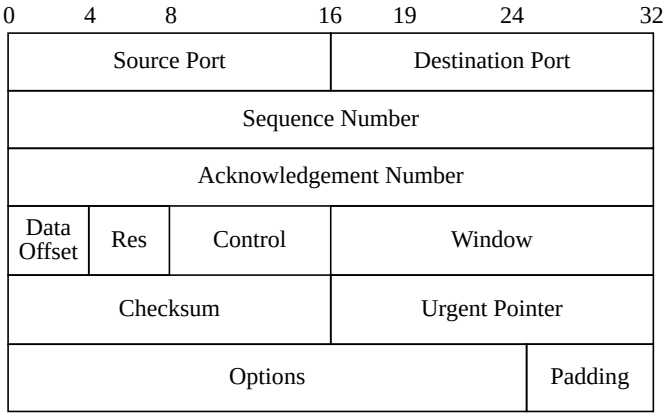


Fig. 16.12 - Header del pacchetto TCP.

16.11 IL PROTOCOLLO UDP

Lo *User Datagram Protocol* (UDP) è un protocollo di trasporto, alternativo a TCP, di tipo connectionless. UDP è un protocollo molto più semplice di TCP ed è utilizzato quando l'affidabilità di TCP non è richiesta.

La struttura del pacchetto UDP è mostrata in figura 16.13. I campi hanno significati simili a quelli di TCP, e la checksum è opzionale.

Un esempio di pacchetto UDP su IP è riportata in appendice B, paragrafo B.3.5.

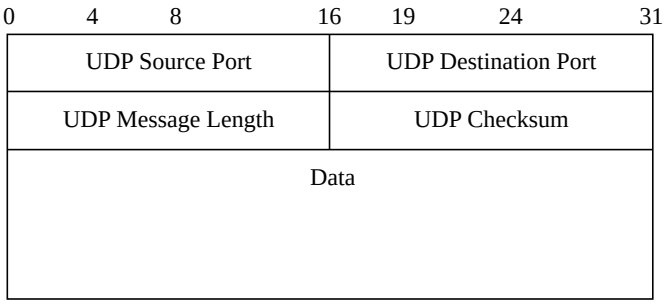


Fig. 16.13 - Il pacchetto UDP.

16.12 GLI APPLICATIVI

16.12.1 Telnet e rlogin

Telnet è un protocollo che permette ad un utente di collegarsi, tramite l'elaboratore locale, ad un qualsiasi altro elaboratore remoto connesso alla rete.

La connessione viene attivata facendo seguire al comando telnet il nome del calcolatore remoto o il suo indirizzo. Da quel momento in poi, tutti i caratteri battuti sulla tastiera sono inviati all'elaboratore remoto e le risposte da questo generate sono visualizzate sullo schermo locale. Il calcolatore locale è reso trasparente dal programma telnet e si opera come se si fosse direttamente connessi all'elaboratore remoto. Quando ci si scollega dall'elaboratore remoto, il programma telnet termina e ci si trova nuovamente a dialogare con il sistema operativo dell'elaboratore locale.

Normalmente il programma telnet include degli emulatori per i terminali più diffusi (es. Digital VT100 e IBM 3270).

Telnet è specificato dagli RFC 854 e 855 ed un esempio di PDU telnet su TCP/IP è riportato in appendice B, paragrafo B.3.1.

Alternativamente al telnet è possibile utilizzare il comando *rlogin* che ha funzionalità analoghe.

16.12.2 FTP, RCP e TFTP

Il *File Transfer Protocol* (FTP) è un applicativo che permette ad un utente collegato ad un elaboratore di trasferire file da e verso un altro elaboratore. La sicurezza è gestita chiedendo all'utente di fornire uno username e una password validi

sull'elaboratore remoto. FTP gestisce anche la conversione automatica di file di testo tra elaboratori con codifiche dei caratteri diverse. FTP è specificato nel RFC 959.

RCP è un applicativo simile a FTP in cui variano i meccanismi di gestione della sicurezza.

TFTP (*Trivial FTP*) è una versione semplificata di FTP usata normalmente per downline loading di software e specificata nel RFC 1350. Un esempio di PDU TFTP su TCP/IP è riportato in appendice B, paragrafo B.3.6.

16.12.3 SMTP

Il *Simple Mail Transfer Protocol* (SMTP) è probabilmente l'applicativo più importante del TCP/IP. Esso permette di inviare posta elettronica agli utenti della rete. Ogni utente è identificato dalla sintassi *Utente@Elaboratore* e non è richiesta alcuna autorizzazione per poter inviare un messaggio di posta elettronica. Il procedimento di invio avviene in batch, riprovando più volte sino a quando l'elaboratore remoto non diventa raggiungibile. L'utente remoto viene avvisato dell'arrivo di un nuovo messaggio.

I principali RFC che si occupano di posta elettronica sono lo RFC 821 e lo RFC 822.

16.12.4 DNS

Il *Domain Name Server* (DNS) è una base di dati distribuita e replicata per gestire principalmente la corrispondenza tra nomi e indirizzi IP. Un esempio di PDU DNS su TCP/IP è riportato in appendice B, paragrafo B.3.7.

Il DNS è specificato negli RFC 1035, 883 e 882.

16.12.5 BOOTP

Il *Boot Protocol* (BOOTP) è un protocollo per il bootstrap via rete di stazioni diskless. Un esempio di PDU BOOTP su TCP/IP è riportato in appendice B, paragrafo B.3.2.

Il BOOTP è specificato nel RFC 951.

16.12.6 ISODE

L'*ISO Development Environment* (ISODE) è un ambiente di sviluppo per applicativi OSI su reti TCP/IP. Un esempio di PDU ISODE su TCP/IP è riportato in appendice B, paragrafo B.3.12.

16.12.7 RSH, REXEC e RWHO

Le applicazioni *rsh* e *rexec* permettono di richiedere che un file di comandi o un programma eseguibile siano eseguiti su un elaboratore remoto invece che sull'elaboratore locale.

L'applicazione *rwho* permette di verificare quali utenti siano connessi da un elaboratore remoto. Un esempio di RWHO PDU su TCP/IP è riportato in appendice B, paragrafo B.3.4.

16.12.8 NFS e Netbios

Il *Network File System* (NFS) è un applicativo di sistema che permette a più elaboratori client di condividere un file system, messo a disposizione da un elaboratore server. Il tipo di network file system più noto è NFS proposto dalla SUN Microsystems ed adottato su tutti gli elaboratori con sistema operativo Unix.

SUN/NFS permette di avere molti server sulla rete e ad ogni elaboratore di fungere contemporaneamente da server e da client, per porzioni diversi del file system. Si appoggia su XDR (*eXternal Data Representation*), un pacchetto con scopi simili al livello Presentation OSI, e questo su RPC (*Remote Procedural Call*) e quindi su UDP e IP. Un esempio di PDU NFS è riportato in appendice B, paragrafo B.3.5.

SUN/NFS richiede una gestione coordinata della sicurezza degli elaboratori coinvolti nel file system distribuito che normalmente è realizzata con l'applicazione di sistema *Yellow Pages* (YP). Un esempio di PDU YP su TCP/IP è riportato in appendice B, paragrafo B.3.10.

Un altro tipo di file system distribuito molto utilizzato in ambito personal computer si basa su Netbios ed è trattato negli RFC 1001 e 1002. Un esempio di PDU Netbios su TCP/IP è riportato in appendice B, paragrafo B.3.11.

16.12.9 SNMP

Il *Simple Network Management Protocol* (SNMP) è un protocollo per la gestione degli apparati, basato su UDP/IP. SNMP è stato progettato per inviare dati sullo stato della rete provenienti dagli apparati ad un centro di gestione che li interpreti in modo opportuno. Con SNMP è anche possibile modificare alcuni parametri degli apparati di rete.

16.12.10 X-Window

X-Window è un software di rete client-server che permette ad un programma client di visualizzare dati grafici del display di un altro elaboratore che funge da server grafico.

Nato nell'ambito del progetto MIT Athena, X-window si è diffuso su tutti gli elaboratori e su tutti i protocolli, tra cui anche TCP/IP. Un esempio di PDU X-window su TCP/IP è riportato in appendice B, paragrafo B.3.8.

16.12.11 NIR

I *Network Information Retrieval* (NIR) sono servizi di tipo ipertestuale, distribuiti, che permettono di accedere ad un'ampia quantità di informazioni in modo semplice, usando un'interfaccia "user friendly" e ignorando dove l'informazione si trovi.

Nati per consentire l'utilizzo della rete Internet anche agli utenti meno esperti, hanno subito avuto un grosso successo e la loro diffusione è stata rapidissima.

Tra questi ricordiamo WAIS, gopher, WWW (Word Wide Web), netfind e X.500. Quest'ultimo è un applicativo nato nel mondo OSI, ma portato in quello Internet tramite ISODE (si veda il paragrafo 16.12.6).

16.12.12 Servizi Multicast

Sono gli ultimi ad essere stati sviluppati nel mondo Internet. Si tratta di servizi di audio e video conferenza basati su TCP/IP che affrontano problematiche nuove, quali quelle della multimedialità su rete. Tra questi ricordiamo Internet Talk Radio, IETF TV e Multimedia, Multiprotocol World.

Nell'ambito di Internet è stata definita una sottorete logica per fornire servizi di video e audio conferenza detta MBONE (*Multicast backBONE*).

BIBLIOGRAFIA

[1] A. Tanenbaum, "Computer Networks," Second Edition, Prentice-Hall.

[2] Douglas E. Comer, "Internetworking with TCP/IP", Volume 1, Second Edition, Prentice-Hall.

[3] L. Hedrick, "Introduction to the Internet Protocol", Rutgers University, New Jersey (USA), 3 July 1993.

[4] T. Socolofsky, C. Kale, "RFC 1180: A TCP/IP Tutorial", January 1991.

[5] Cisco Systems, "Internetworking Technology Overview", Codice documento DOC-ITO13 78-1070-01, 1993.

[6] Cisco Systems, "Router Products Configuration and Reference", Cisco Systems DOC-R9.1, Menlo Park CA (USA), September 92.

[7] M. K. Johnson, "Implementation Detail of the Microsoft LAN Manager TCP/IP Protocol", Microsoft Technical Note, Volume X, Number Y, March 1992.

[8] J. Postel, "RFC 768: User Datagram Protocol", 08/28/1980.

[9] J. Postel, "RFC 791, Internet Protocol", 09/01/1981.

[10] J. Postel, "RFC 792: Internet Control Message Protocol", 09/01/1981.

[11] J. Postel, "RFC 793: Transmission Control Protocol", 09/01/1981.

[12] J. Postel, "RFC 821: Simple Mail Transfer Protocol", 08/01/1982.

[13] D. Crocker, "RFC 822: Standard for the format of ARPA Internet text messages", 08/13/1982.

[14] D. Plummer, "RFC 826: Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", 11/01/1982.

[15] J. Postel, J. Reynolds, "RFC 854: Telnet Protocol specification".

[16] J. Postel, J. Reynolds, "RFC 855: Telnet option specifications".

[17] P. Mockapetris, "RFC 882: Domain names: Concepts and facilities", 11/01/1983.

[18] P. Mockapetris, "RFC 883: Domain names: Implementation specification", 11/01/1983.

[19] International Telegraph and Telephone Co, D. Mills, "RFC 904: Exterior Gateway Protocol formal specification", 04/01/1984.

[20] J. Mogul, J. Postel, "RFC 950: Internet standard subnetting procedure", 08/01/1985.

[21] W. Croft, J. Gilmore, "RFC 951: Bootstrap Protocol", 09/01/1985.

[22] J. Postel, J. Reynolds, "RFC 959: File Transfer Protocol", 10/01/1985.

[23] Defense Advanced Research Projects Agency, End-to-End Services Task Force, Internet Activities Board, NetBIOS Working Group, "RFC 1001: Protocol standard for a NetBIOS service on a TCP/UDP transport: Concepts and methods", 03/01/1987.

[24] Defense Advanced Research Projects Agency, End-to-End Services Task Force, Internet Activities Board, NetBIOS Working Group, "RFC 1002: Protocol standard for a NetBIOS service on a TCP/UDP transport: Detailed specifications", 03/01/1987.

[25] P. Mockapetris, "RFC 1035: Domain names - implementation and specification", 11/01/1987.

[26] C. Hedrick, "RFC 1058, RIP: Routing Information Protocol", 06/01/1988.

[27] S. Deering, "RFC 1112: Host extensions for IP multicasting", 08/01/1989.

[28] K. Lougheed, Y. Rekhter, "RFC 1267: A Border Gateway Protocol 3 (BGP-3)", 10/25/1991.

[29] K. Sollins, "RFC 1350: The TFTP protocol (revision 2)", 07/10/1992.

[30] G. Malkin, "RFC 1388: RIP Version 2 Carrying Additional Information", 01/06/1993.

[31] J. Moy, "RFC 1583: OSPF Version 2", 03/23/1994.

[32] Hinden, "RFC 1517: Applicability Statement for the Implementation of Classless Inter-Domain Routing (CIDR)", 09/24/1993.

[33] Rekhter, T. Li, "RFC 1518: An Architecture for IP Address Allocation with CIDR", 09/24/1993.

[34] Fuller, T. Li, J. Yu, K. Varadhan, "RFC 1519: Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy", 09/24/1993.

[35] Rekhter, C. Topolcic, "RFC 1520: Exchanging Routing Information Across Provider Boundaries in the CIDR Environment", 09/24/1993.

17

L'ARCHITETTURA DI RETE OSI

17.1 INTRODUZIONE

L'ISO ha completato il modello di riferimento OSI (*Open System Interconnection*) nel 1984 ed esso è oggi universalmente accettato. La realizzazione di una architettura di rete totalmente conforme a tale modello ha richiesto invece molto più tempo e solo dieci anni dopo si sono iniziate ad avere le prime realizzazioni di reti OSI.

L'architettura di una rete OSI è mostrata in figura 17.1.

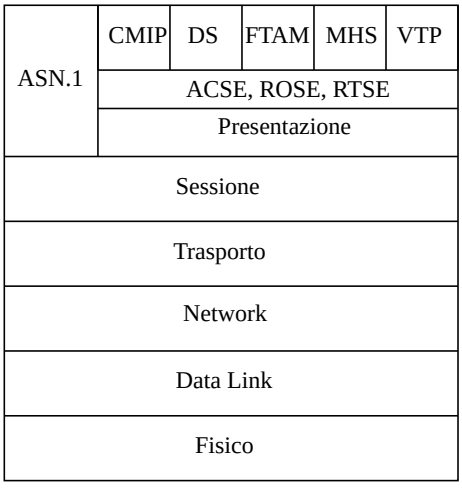


Fig. 17.1 - Architettura di una rete OSI.

17.1.1 I livelli 1 e 2

Gli standard OSI per il livello 1 (Fisico) e 2 (Data Link) sono universalmente accettati e sono descritti nei capitoli dal 5 al 13.

17.1.2 Il livello 3

Il livello 3 OSI (Network) è indubbiamente il livello chiave per la diffusione di OSI. L'accettazione di tale livello per tutte le architetture di rete porterebbe ad una grande razionalizzazione delle problematiche di internetworking. Il livello 3 OSI è descritto in modo approfondito nel seguito di questo capitolo.

17.1.3 Il livello 4

Il livello 4 OSI (Transport) prevede cinque possibili protocolli di trasporto detti TP0, TP1, TP2, TP3 e TP4. I primi quattro assumono che il livello 3 sia connesso, mentre TP4 può operare su un livello 3 sia connesso che non connesso.

TP0 è il più semplice ed effettua solo frammentazione e riassemblaggio dei pacchetti. TP1 aggiunge a questo anche un meccanismo base di correzione degli errori.

TP2 è in grado di utilizzare un singolo circuito virtuale di livello 3 per più flussi dati di livello 4. Questo è particolarmente utile se la rete di livello 3 è una rete a commutazione di pacchetto pubblica, con un numero limitato di circuiti virtuali.

TP3 unisce le caratteristiche di TP1 e TP2.

TP4 è il protocollo OSI più comunemente usato. Esso è molto simile al protocollo TCP dell'architettura TCP/IP. Aggiunge alle caratteristiche del TP3 la possibilità di operare su un livello 3 non connesso, fornendo un trasporto affidabile dell'informazione.

17.1.4 Il livello 5

Il livello 5 OSI (Session) è il livello sessione, responsabile dell'organizzazione del dialogo tra due programmi applicativi e del conseguente scambio di dati. Esso consente di aggiungere, ai servizi forniti dal trasporto, servizi più avanzati, quali la gestione del dialogo (mono o bidirezionale), la gestione del token (per effettuare mutua esclusione) o la sincronizzazione (inserendo dei checkpoint in modo da ridurre la quantità di dati da ritrasmettere in caso di gravi malfunzionamenti).

17.1.5 Il livello 6

Il livello 6 OSI (Presentation) è il livello presentazione, che gestisce la sintassi dell'informazione da trasferire. A questo livello sono previste tre diverse sintassi: astratta (definizione formale dei dati che gli applicativi si scambiano, come in ISO 8824 o in ASN.1), concreta locale (come i dati sono rappresentati localmente) e di trasferimento (come i dati sono codificati durante il trasferimento).

17.1.6 Il livello 7

Il livello 7 OSI (Application) include, oltre alle applicazioni, anche gli ASE (*Application Service Element*) che facilitano la comunicazione tra gli applicativi e i livelli inferiori. Gli ASE più importanti sono:

- *ACSE (Association Control Service Element*). ACSE fornisce le associazioni tra nomi che sono alla base delle comunicazioni di tipo application-to-application.
- *ROSE (Remote Operation Service Element).* ROSE implementa una modalità operativa simile a quella delle RPC (Remote Procedural Call) di TCP/IP.
- *RTSE (Reliable Transfer Service Element).* RTSE serve a migliorare l'affidabilità nella trasmissione delle informazioni.

Gli applicativi standard sono:

- *VTP (Virtual Terminal Protocol).* È il protocollo che fornisce l'emulazione terminale in modo simile al telnet del TCP/IP.
- *FTAM (File Transfer, Access and Management).* È il protocollo per il file transfer tra sistemi. Rispetto a FTP di TCP/IP è più sofisticato, in quanto incorpora anche concetti derivati dai file system distribuiti.
- *MHS (Message Handling System).* È il protocollo per la posta elettronica, pensato per avere una struttura sofisticata, con allegati di vario tipo, anche binari e quindi anche multimediali. Lo standard OSI per questo applicativo è lo X.400.
- *DS (Directory Service).* È lo standard per un database globale distribuito di tutti gli utenti di rete, con un indirizzamento di tipo "postale". Lo standard OSI per questo applicativo è X.500, ma il DS si è già diffuso anche sulle reti TCP/IP.

17.2 IL LIVELLO 3 OSI

I servizi forniti dal livello 3 OSI sono descritti nello standard *ISO 8348, network service definition.*

Durante la fase di specifica di questo livello si è assistito ancora una volta alla disputa tra i sostenitori della modalità connessa e quelli della modalità non connessa.

Il risultato finale è stato l'accettazione di entrambe le modalità e la produzione di due gruppi di standard, uno per la modalità connessa e l'altro per quella non connessa.

Nel seguito di questo capitolo verranno discusse le problematiche generali del routing OSI e verrà approfondita la descrizione della modalità non connessa in quanto è quella adottata dall'architettura di rete DECnet fase V, la prima importante utilizzatrice del routing OSI.

17.3 PROTOCOLLI CONNESSI

La modalità connessa (CONS) del livello 3 OSI si basa sull'utilizzo di X.25. Due standard principali definiscono l'utilizzo di tale modalità:

- *ISO 8208, X.25 packet-level protocol for Data Terminal Equipment*. Questo standard è la versione ISO della raccomandazione CCITT X.25. ISO 8208 definisce l'interfaccia tra un elaboratore ed una rete a commutazione di pacchetto X.25. ISO 8208 non definisce un servizio CONS, ma lo deriva dalle caratteristiche intrinseche delle reti X.25. Si noti che le reti X.25 sono adatte a supportare il protocollo OSI CONS solo se conformi alla versione X.25-1984 o a versioni successive. La versione 1990 non ha tutte le primitive richieste.
- *ISO 8878, Use of X.25 to provide the OSI connection-mode network service.* Questo standard aggiunge delle funzionalità allo standard precedente fornendo tutte le primitive necessarie a realizzare un servizio OSI CONS. ISO 8878 può essere pensato come uno strato che si appoggia su ISO 8208 e definisce come il servizio OSI CONS è realizzato a partire dalle funzionalità di una rete X.25.

Occorre sottolineare che il routing OSI CONS integra al suo interno le potenzialità di instradamento delle reti X.25. Quando un pacchetto OSI transita su una rete X.25, esso ha una sola busta di livello 3, quella X.25.

Questo non è vero per architetture quali DECnet fase IV o TCP/IP, in cui la rete X.25 viene vista solo come una realtà esterna che consente di creare dei canali virtuali punto-punto tra due router (detti DLM in terminologia DECnet fase IV, si veda 15.2.2). Quando un pacchetto appartenente a queste architetture transita su una rete

X.25, ha due buste di livello 3: quella di X.25 e quella proprietaria dell'architettura (ad esempio, quella IP).

Per una comparazione tra la modalità connessa e quella non connessa si veda il paragrafo 14.2; per una trattazione ancora più approfondita si consultino [2, 3].

17.4 PROTOCOLLI NON CONNESSI

La modalità non connessa (CLNS) OSI si basa su quattro standard principali:

- *ISO 8473, Protocol for providing the connectionless-mode network service*. Questo è il protocollo che trasporta i dati di utente in modalità non connessa. È spesso detto anche ISO IP (Internet Protocol) per la sua somiglianza con il protocollo IP dell'architettura TCP/IP, con cui però è incompatibile. È stato progettato per la trasmissione di dati tra due End System (ES) connessi attraverso un numero arbitrario di sottoreti e Intermediate System (IS) di vario tipo.
- *ISO 9542, End system to Intermediate system routing exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473).* Questo protocollo, detto per brevità ES-IS, è il protocollo con cui gli ES e gli IS si scambiano informazioni utili per il routing. In particolare, ES-IS tratta le problematiche di neighbor greetings e di routing redirect. Inoltre questo protocollo permette ad un ES di autoconfigurarsi scambiando informazioni di configurazione con gli IS (i router).
- *ISO 10589, Intermediate system to intermediate system intra-domain routing exchange protocol for use in conjunction with the protocol for providing CLNS (ISO 8473).* Questo protocollo, detto per brevità IS-IS, è il protocollo con cui gli IS si scambiano informazioni utili per il routing. In particolare IS-IS è utilizzato dagli IS per costruire le tabelle di instradamento utilizzando un algoritmo di tipo Link State Packet.
- *ISO 10747, Protocol for exchange of inter-domain routing information among intermediate systems to support forwarding of ISO 8473 PDUs*. Questo protocollo, detto per brevità IDRP (Inter Domain Routing Protocol), è il protocollo con cui IS appartenenti a domini di routing diversi si scambiano informazioni di raggiungibilità. ISO IDRP è derivato dal protocollo BGP di TCP/IP.

17.5 ISO 8473 - CLNS

Il protocollo ISO 8473 definisce due tipi di PDU:

- *data packet*. Sono i pacchetti più comuni che trasportano l'informazione tra due ES che stanno comunicando attraverso il livello 3.
- *error report packet*. È un pacchetto che segnala una condizione di errore, verificatasi durante la trasmissione di un data packet, al nodo mittente del data packet. È generato dal nodo che ha scartato il data packet.

La figura 17.2 mostra l'header del pacchetto ISO 8473, valido per entrambi i tipi di pacchetti.

Ottetti					
1	network layer protocol identifier				
1	length indicator				
1	version/protocol ID extension				
1	lifetime				
1	SP	MS	ER	type	
2	segment length				
2	header checksum				
1	destination address length				
1 - 20	destination address				
1	source address length				
1 - 20	source address				
2 o non presente	data unit identifier				
2 o non presente	segment offset				
2 o non presente	total length				
variabile	option				

Fig. 17.2 - Il pacchetto ISO 8473.

Il significato dei vari campi è il seguente:

- *Network layer protocol identifier*. È un identificatore del protocollo. Vale 129 (81H) per ISO 8473, 130 (82H) per ES-IS e 131 (83H) per IS-IS.
- *Length indicator*. È la lunghezza dell'header in ottetti.
- *Version/protocol ID extension*. Contiene il valore 1.

- *Lifetime*. Questo campo viene inizializzato ad un valore diverso da zero dal mittente. Esprime la vita residua del pacchetto in unità di tempo pari a 1/2 secondo. Ogni router deve decrementarlo di almeno un'unità, in funzione del ritardo introdotto. Quando questo campo raggiunge il valore zero, il pacchetto viene scartato.
- *SP (Segmentation Permitted).* Se questo bit è a 1 il pacchetto può essere frammentato.
- *MS (More Segment).* È un bit a 1 in tutti i frammenti eccetto l'ultimo.
- *ER (Error Report).* Questo bit, quando posto uguale a 1, indica che il mittente vorrebbe essere informato, se possibile, se il pacchetto non può essere recapitato.
- *Type*. È il tipo del pacchetto: 28 indica un data packet, 1 indica un error report packet.
- *Segment length*. È la lunghezza complessiva (header + dati) del pacchetto in ottetti.
- *Header checksum*. Due checksum diverse da 8 bit usate per verificare l'integrità dell'header. Se a zero indicano che la checksum non è utilizzata.
- *Destination address length e destination address*. Contengono rispettivamente la lunghezza dell'indirizzo di destinazione e l'indirizzo di destinazione (per il formato si veda 17.8).
- *Source address length e source address*. Contengono rispettivamente la lunghezza dell'indirizzo di mittente e l'indirizzo di mittente (per il formato si veda 17.8).
- *Data unit identifier*. Questo campo è presente solo se il bit SP è a 1. È un numero assegnato al pacchetto, prima di frammentarlo, con lo scopo di semplificare l'operazione di riassemblaggio dei frammenti.
- *Segment offset*. Questo campo è presente solo se il bit SP è a 1. È l'offset del frammento in ottetti.
- *Total length*. Questo campo è presente solo se il bit SP è a 1. È la lunghezza complessiva del pacchetto (header + dati) prima della frammentazione.
- *Option*. Una serie vasta di opzioni che includono il padding, la sicurezza, il source routing, il route recording (registrazione dei router attraversati), la qualità del servizio, la priorità e la ragione per cui un pacchetto è stato scartato.

Esistono anche due versioni semplificate del protocollo ISO 8473:

- *Inactive network layer subset*. Si può utilizzare quando è noto a priori che sia il mittente sia il destinatario appartengono alla stessa sottorete fisica.
- *Nonsegmenting subset*. Si può utilizzare quando è noto a priori che non sarà necessario segmentare il pacchetto per attraversare le sottoreti fisiche che connettono il mittente al destinatario.

17.6 GERARCHIA

Le reti OSI hanno una struttura di tipo gerarchico, illustrata in figura 17.3. Si noti che i due livelli più esterni fanno riferimento a gerarchie unicamente amministrative e non hanno quindi impatto a livello di protocolli di rete.

Una rete OSI è quindi un insieme di *domini* (equivalenti agli Autonomous System di TCP/IP), ciascuno composto da una o più *aree* (equivalenti alle aree DECnet fase IV o alle network IP), composte a loro volta da ES e IS.

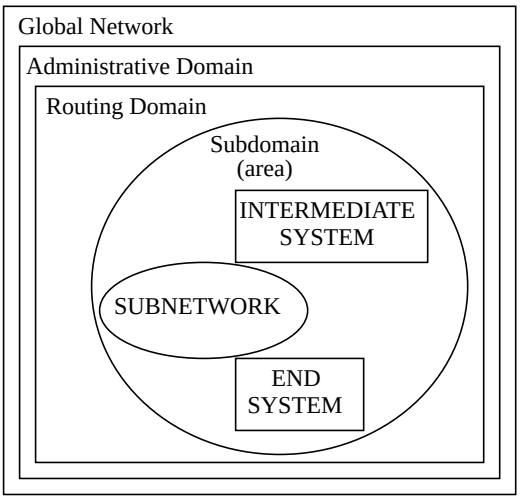


Fig. 17.3 - Modello di gerarchia in OSI.

La figura 17.4 mostra un esempio di una rete OSI formata da un solo dominio di routing, interconnesso con altri domini. Il dominio è a sua volta composto da quattro aree e per i router (IS) si adotta una terminologia molto simile a quella di DECnet fase IV.

Si noti che la distinzione tra aree diverse è implicita nel formato dell'indirizzo, così come avviene in TCP/IP per le network. La distinzione tra domini diversi invece non è strutturale nel formato dell'indirizzo, analogamente a quanto avviene in TCP/IP per gli Autonomous System.

I domini sono delle aggregazioni di aree definite a livello di router. Una stessa rete può essere progettata per avere un solo dominio o più domini. Nel caso di più domini, saranno i router IDRP a sapere quali aree appartengono a quali domini.

I router intra-area utilizzano una sola copia dell'algoritmo IS-IS (ISO 10589) in quanto conoscono solo i nodi interni all'area, mentre i router di area usano due copie dell'algoritmo IS-IS, una relativa alla loro area di appartenenza, l'altra di tipo inter-

area che considera tutti i router di livello 2 e le loro interconnessioni.

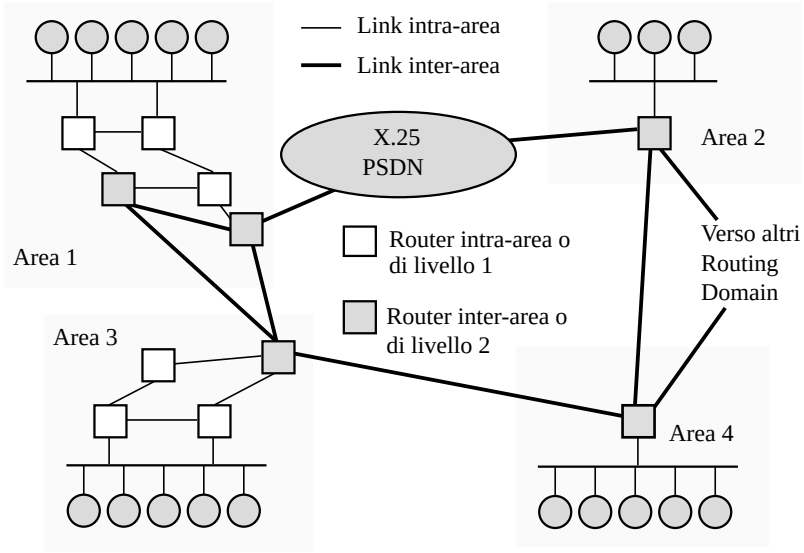


Fig. 17.4 - Esempio di rete OSI.

Quando un router di livello 1 deve inviare un messaggio ad un'altra area, lo invia al più vicino router di livello 2 appartenente alla sua area. Questa informazione è nota ai router di livello 1 in quanto nei LSP c'è un campo che indica il livello di ogni nodo.

Un router di livello 2 può anche operare come router inter-dominio e allora, oltre alle due copie dell'algoritmo IS-IS, usa anche una copia dell'algoritmo IDRP (ISO 10747).

17.7 NEIGHBOR GREEETINGS

Le problematiche di *neighbor greetings* sono affrontate dal protocollo ISO 9542 ES-IS.

Usando tale protocollo ogni ES annuncia la propria presenza periodicamente trasmettendo dei pacchetti ESH (*End System Hello*) ad uno speciale indirizzo di gruppo riconosciuto dai soli router. Analogamente, gli IS trasmettono periodicamente pacchetti ISH (*Intermediate System Hello*) ad un indirizzo di gruppo riconosciuto dai soli ES.

Gli ES sono dotati di due cache: una *router cache* e una *destination cache*. Queste cache sono degli insiemi di triplette del tipo {indirizzo di livello 3, indirizzo di livello 2, tempo}, dove l'informazione di tempo è utilizzata per limitare la validità temporale di ciascuna tripletta.

Gli ES ascoltano gli ISH e li memorizzano nella loro router cache.

Quando un mittente M deve trasmettere ad un destinatario D compie le seguenti azioni:

- Se D è nella destination cache, M trasmette il pacchetto all'indirizzo di livello 2 corrispondente.
- Se D non è nella destination cache e c'è almeno un router nella router cache, allora M trasmette il pacchetto ad un router qualsiasi, specificando come indirizzo di livello 2 quello del router.
- Se D non è nella destination cache e la router cache è vuota (non esistono router sulla LAN), allora M trasmette il pacchetto multicast a tutti gli ES. D accetta il pacchetto e trasmette il suo ESH ad M che lo inserisce nella destination cache.

Quando un router si trova a dover instradare un pacchetto sulla stessa linea da cui lo ha ricevuto genera un messaggio di routing redirect indirizzato al nodo M. Quando M riceve il routing redirect aggiorna la destination cache con l'indirizzo di livello 2 indicato nel messaggio dal router.

17.8 INDIRIZZAMENTO

Gli indirizzi OSI sono lunghi sino a 20 ottetti, hanno una struttura piuttosto articolata e vengono indicati con la sigla NSAP (*Network Service Access Point*) o, più raramente, NET. Essi sono specificati nello standard *ISO 8348 amendment 2: network layer addressing*.

Dal punto di vista dei router, essi sono composti da tre parti: Area, Node ID e SEL (figura 17.5e).

Il campo *Node ID* è l'indirizzo del nodo all'interno della sottorete fisica, quindi, sulle LAN, l'indirizzo MAC della stazione. Il campo Node ID può essere visto anche come l'indirizzo dell'host all'interno dell'area.

Il campo *Area* è l'indirizzo dell'area, cioè della sottorete logica di livello 1 all'interno della quale il nodo risiede.

Il campo *SEL* serve ad indicare chi è l'utente del livello Network, permettendo a più protocolli di trasporto, anche non compatibili con OSI, di appoggiarsi sul livello Network OSI (figura 17.6).

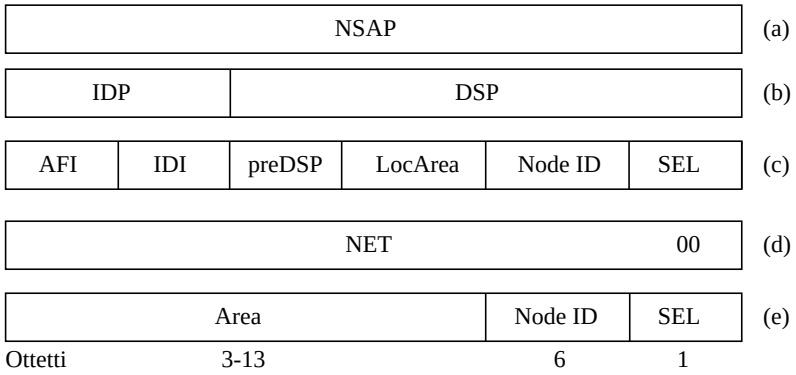


Fig. 17.5 - NSAP e NET.

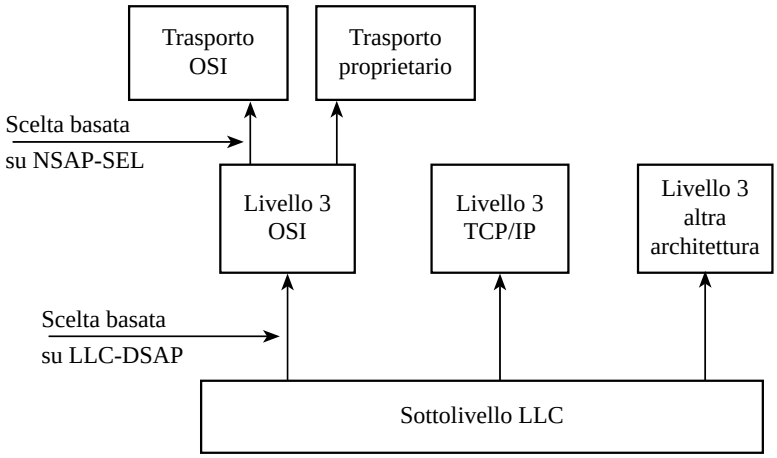


Fig. 17.6 - Il campo SEL.

I valori attualmente assegnati al campo SEL (selector) sono: 32 (20H) per il trasporto OSI, 33 (21H) per il trasporto NSP (DECnet fase IV) e 00 per indicare il livello network stesso. Quest'ultimo valore è stato introdotto per razionalizzare l'uso di due concetti presenti a livello 3: NSAP e NET.

Il NSAP indica i punti di accesso a cui il livello 4 può ottenere servizi dal livello 3 e non può quindi considerarsi a tutti gli effetti un indirizzo del livello 3. Quest'ultimo è definito dallo standard essere il NET (*Network Entity Title*). La relazione esistente tra i due è che NET si ottiene da NSAP ponendo il campo SEL uguale a zero (figure

17.5a e 17.5d).

Gli indirizzi OSI sono garantiti essere univoci a livello mondiale e sono assegnati, esplicitamente o implicitamente, da sei diverse autorità. Esiste un settimo tipo di indirizzi per uso privato.

Quando si analizza il processo di assegnazione degli indirizzi occorre dettagliarne maggiormente la struttura. Un indirizzo OSI può essere visto come costituito da due parti (figura 17.5b): l'*Initial Domain Part* (IDP) e la *Domain Specific Part* (DSP).

Queste due parti si suddividono a loro volta in altre parti (17.5c): l'*Authority and Format Identifier* (AFI), l'*Initial Domain Identifier* (IDI), il *Prefix to the DSP* (PreDSP), la *Local Area* (LocArea), oltre ai già discussi Node ID e SEL.

17.8.1 AFI

Questo campo identifica l'autorità che ha assegnato l'indirizzo e il formato dell'indirizzo stesso. Il campo AFI consiste in due cifre decimali: alcuni possibili valori sono riportati in tabella 17.1.

Autorità	AFI	Numero Max. Cifre in IDI	Utilizzare questo AFI se la prima cifra dell'IDI è	Numero max. Cifre nel preDSP
Private	49	0		20
ISO DCC	39	3		16
ISO 6523-ICD	47	4		16
X.121	37 53	massimo 14	non zero zero	6
F.69	41 55	massimo 8	non zero zero	12
E.163	43 57	massimo 12	non zero zero	8
E.164	45 59	massimo 15	non zero zero	4

Tab. 17.1 - Autorità e formati per NSAP.

L'autorità che assegna gli indirizzi può essere:

- *Private*. Nessuna autorità, scelta privata degli indirizzi.

- *ISO DCC*. Indirizzi assegnati dall'ISO esplicitamente su base nazionale. Il campo IDI contiene l'identificativo della nazione (tabella 17.2). Questi indirizzi in Italia sono assegnati dall'UNINFO*.
- *ISO ICD*. Indirizzi assegnati dall'ISO esplicitamente su base internazionale. Il campo IDI contiene l'identificativo dell'organizzazione cui è stato assegnato l'indirizzo.
- *X.121*. Indirizzi assegnati implicitamente dal CCITT. Il campo IDI contiene un indirizzo X.25 pubblico, cioè in Italia un indirizzo di Itapac.
- *F.69*. Indirizzi assegnati implicitamente dal CCITT. Il campo IDI contiene un numero di Telex.
- *E.163*. Indirizzi assegnati implicitamente dal CCITT. Il campo IDI contiene un numero di telefono.
- *E.164*. Indirizzi assegnati implicitamente dal CCITT. Il campo IDI contiene un numero ISDN.

Nazione	Sigla	IDI
Australia	AU	036
Austria	AT	040
Belgio	BE	056
Canada	CA	124
Danimarca	DK	208
Francia	FR	250
Germania	DE	280
Italia	IT	380
Giappone	JP	392
Olanda	NL	528
Spagna	ES	724
Regno Unito	GB	826
Svizzera	CH	756
USA	US	840

Tab. 17.2 - ISO 3166: Nazioni principali.

* UNINFO, Commissione Tecnica Unificazione, Corso Galileo Ferraris, 93 - 10128 Torino, Tel. 011/501027, 011/501837.

17.8.2 PreDSP

Questo campo si usa in congiunzione con gli indirizzi ISO DCC e ICD. A livello di ISO DCC si usa per identificare l'organizzazione all'interno della nazione. Il suo formato è definito a livello nazionale. Nel seguito verranno mostrati i formati americano e italiano del PreDSP, quando usato in un indirizzo ISO DCC.

17.8.3 PreDSP USA

L'ANSI ha suddiviso le 16 cifre del PreDSP in 4 campi:

- *DFI (DSP Format Identifier).* Consiste in due cifre esadecimali che indicano il formato usato per gli altri campi del PreDSP. Il valore 80 indica il formato US GOSIP.
- *ORG (Organization ID).* Consiste in 6 cifre esadecimali che indicano l'organizzazione all'interno della nazione.
- *RES (Reserved).* Consiste in 4 cifre decimali sempre a zero.
- *RD (Routing Domain).* Indica il dominio di routing all'interno dell'organizzazione. Consiste in 4 cifre esadecimali. Consente di semplificare l'identificazione dei routing domain da parte dei router.

17.8.4 PreDSP Italia

La descrizione del PreDSP italiano si basa su una bozza elaborata dal GARR (Gruppo Armonizzazione Reti per la Ricerca). La sua struttura è mostrata in figura 17.7.

Fig. 17.7 - PreDSP italiano.

Il significato dei campi è il seguente:

- *IT-DP (Italian Domain Part).* È la parte di PreDSP che identifica il formato e l'organizzazione.

– *IT-FI (Italian Format Identifier).* È l'identificatore di formato e ha lunghezza di un ottetto. I valori leciti sono riportati in tabella 17.3. La notazione /xx indica che le cifre xx sono in esadecimale.
– *IT-DI (Italian Domain Identifier).* È l'identificatore dell'organizzazione.
– *ORG-DSP (Organization DSP).* Lo standard italiano lascia libertà sull'utilizzo di questo campo all'interno dell'organizzazione, fatto salvo che gli ultimi 9 ottetti sono: LocArea (2 ottetti), Node Id (6 ottetti) e SEL (1 ottetto).

Valore IT-FI	Lunghezza IT-DI	Lunghezza ORG-DSP	Utilizzatori
/10	1 ottetto	15 ottetti	grandi organizzazioni o fornitori di servizi di rete
/20	2 ottetti	14 ottetti	medie organizzazioni
/30	4 ottetti	12 ottetti	piccole organizzazioni
/80	3 ottetti	13 ottetti	organizzazioni che vogliono seguire il formato US GOSIP

Tab. 17.3 - Valori IT-FI.

17.8.5 NSAP: scrittura e visualizzazione

I NSAP possono essere scritti in due formati diversi. Il formato più comprensibile è quello di DNA (DECnet fase V) che interpone il carattere ":" tra i vari campi, mentre OSI interpone il carattere "+" solo tra IDP e DSP.

Il formato DNA è aa:iii...ii:pp-p...p-pp-ll-ll:nn-nn-nn-nn-nn-nn:ss.

Il formato OSI è aaiii...ii+ppp...pppllllnnnnnnnnnnnn:ss

dove:

- aa è il valore del campo AFI in decimale;
- ii.. è il valore del campo IDI in decimale;
- pp... è il valore del campo preDSP in esadecimale;
- ll... è il valore del campo LocArea in esadecimale;
- nn.. è il valore del campo Node ID in esadecimale;
- ss è il valore del campo SEL in esadecimale.

17.8.6 Esempio 1: DCC USA

NSAP in formato DNA: 39:840:80-01-e2-40-00-00-00-00-00-01:02-00-3a-23-12-7f:20.

NET in formato DNA: 39:840:80-01-e2-40-00-00-00-00-00-01:02-00-3a-23-12-7f:20.

NSAP in formato OSI: 39840+8001e240000000000000102003a23127f20.

Si tratta di un indirizzo DCC in quanto AFI = 39 (tabella 17.1). È stato assegnato negli USA in quanto IDI = 840 (tabella 17.2). Il preDSP è uguale a 80-01-e2-40-00-00-00-00, mentre LocArea è uguale a 00-01. Il Node ID è l'indirizzo MAC della stazione 02-00-3a-23-12-7f, mentre il campo SEL vale 20 e indica il trasporto OSI.

Analizzando più nel dettaglio il PreDSP, si vede che esso è il formato US GOSIP (DFI = 80), che l'organizzazione è identificata da 01-e2-40, che il campo reserved è correttamente a 00-00 e che il routing domain è 00-00.

17.8.7 Esempio 2: DCC Italia

Esempio di NSAP: 39:380:20-07-01-00-00-00-00-00-04-00:08-00-2B-13-06-11:20

Questo NSAP identifica una organizzazione di medie dimensioni (IT-FI = 20), cui è stato assegnato un IT-DI uguale a 07-01. Il valore di LocArea è 04-00.

17.8.8 Esempio 3: Indirizzo privato

Esempio di NSAP in formato DNA: 49::00-10:08-00-2b-3c-11-4e:21.

Esempio di NSAP in formato OSI: 49+001008002b3c114e21.

L'indirizzo non è assegnato da una autorità (AFI = 49), appartiene all'area 16 (10 esadecimale), corrisponde alla stazione con indirizzo MAC 08-00-2b-3c-11-4e e indirizza un trasporto NSP (DECnet fase IV).

17.8.9 Esempio 4: Numero telefonico

Si consideri un numero di Roma:

- prefisso internazionale per l'Italia: 39;
- prefisso di Roma: 6;
- numero telefonico: 45678901;

- LocArea: 00-1F;
- indirizzo MAC della stazione: 08-00-00-45-78-FE;
- trasporto OSI.

Lo NSAP risultante è: 43:39645678901:00-1F:08-00-00-45-78-FE:20.

17.8.10 Esempio 5: ICD Nordunet

Esempio di NSAP: 47:0023:80-00-00-55-00-00-00-00-00-03:02-00-00-45-89-65:21.

Il valore 0023 è l'identificativo assegnato da ISO a Nordunet.

17.8.11 Esempio 6: DCC Svizzero

Esempio di NSAP: 39:756:80-11-11-15-00-00-00-00-01-03:02-00-00-45-89-65:20.

Questo NSAP identifica una organizzazione svizzera (IDI = 756) che vuole seguire il formato US GOSIP (CH-FI = 80). L'organizzazione ha CH-DI = 11-11-15 (Hoffmann-La Roche) e il valore di LocArea è 01-03.

17.8.12 Esempio 7: Indirizzo X.25

L'IDI è lungo al massimo 14 cifre di cui 4 sono il DNIC (Data Network Identification Code), 8 sono il numero nazionale e 2 un sottoindirizzo gestito dall'utente.

Esempio di NSAP: 37:81072678789611:01-78:08-00-2b-78-90-11:20.

Dove:

- 37 identifica un NSAP di tipo X.121;
- 8107 è il prefisso internazionale della rete X.25;
- 2678789654 è il numero di DTE nazionale;
- 11 è il sottoindirizzo privato;
- 01-78 è LocArea;
- 08-00-2b-78-90-11 è l'indirizzo MAC della stazione;
- 20 indica il trasporto OSI.

17.9 ALTRE CARATTERISTICHE DEL LIVELLO 3 OSI

Le caratteristiche sino a qui descritte sono quelle principali del livello 3 OSI. Ne sono presenti molte altre e per una trattazione approfondita si consulti [2, 3].

Tuttavia, meritano essere menzionati il multi-link ES, l'autoconfigurazione e il multi-homing.

17.9.1 Multi-link ES

Si tratta di ES che hanno più di un collegamento di rete attivo contemporaneamente, ma che continuano a rimanere ES (figura 17.8).

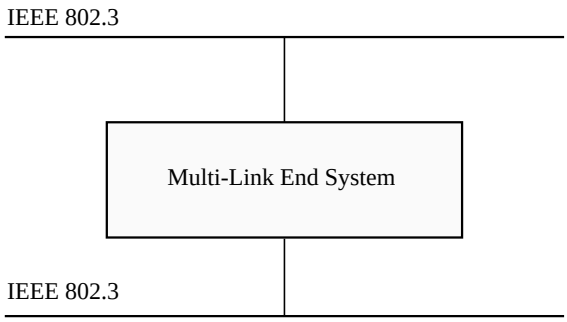


Fig. 17.8 - Multi-link ES.

Questo non è normalmente possibile in altre architetture di rete in quanto, quando un nodo ha più di un collegamento, assume automaticamente la funzionalità di router.

L'utilità dei *multi-link ES* è quella di aumentare l'affidabilità e le prestazioni dell'ES. Infatti, in impianti in cui è richiesta un'elevata affidabilità, disporre al massimo di un collegamento alla rete locale per ogni nodo è difficilmente accettabile.

17.9.2 Autoconfigurazione

Gli ES OSI possono autoconfigurare il loro indirizzo di livello 3 tramite il protocollo IS-ES. Infatti l'indirizzo di un ES e di un IS connessi alla stessa rete locale differiscono solo nel campo Node ID.

L'ES può autoconfigurare il suo indirizzo prendendo quello del router e sostituendo il campo Node ID con il suo indirizzo MAC, scritto sulla ROM della scheda di rete locale.

17.9.3 Multi-homing

Una rete fisica può avere più indirizzi logici, cioè i suoi sistemi possono essere configurati per rispondere a più NSAP diversi (figura 17.9).

Questo è particolarmente utile, ad esempio, quando una rete fa parte di una rete aziendale, ma è anche connessa ad una rete pubblica. Allora si chiede ai nodi di rispondere a due indirizzi diversi, uno con la parte di Area corrispondente alla rete aziendale (es: Area #1) e l'altro con la parte di Area corrispondente alla rete pubblica (es: Area #2).

Chiaramente, per ogni ES la parte Node ID è uguale nei due indirizzi, invece varia la parte di Area, intesa come in figura 17.5e.

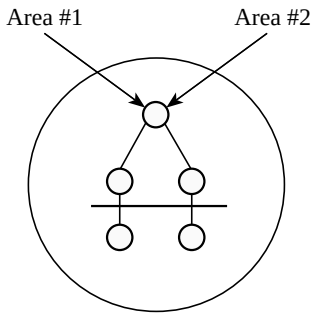


Fig. 17.9 - Sistemi multi-homed.

BIBLIOGRAFIA

[1] Cisco Systems, "Internetworking Technology Overview", Codice documento DOC-ITO13 78-1070-01, 1993.

[2] J. Martin, J. Leben, "DECnet Phase V: An OSI Implementation", Digital Press, Bedford MA (USA), 1992.

[3] R. Perlman, "Interconnections: Bridges and Routers", Addison Wesley, Reading MA (USA), 1992.

[4] IS 8348, "Information Technology - Open Systems Interconnection - Network Service Definition", ISO, 1993.

[5] DAM 8348, "Amendment 1: Connectionless-mode Transmission", ISO.

[6] DAM 8348, "Amendment 2: Network Layer Addressing", ISO.

[7] DAM 8348, "Amendment 3: Additional Features of the Network Service", ISO.

[8] DAM 8348, "Amendment 5: Group Network addressing", ISO.

[9] IS 8880-1, "Information technology - Telecommunications and information exchange between systems - Protocol combinations to provide and support the OSI Network Service", Part 1: General principles, ISO, 1990.

[10] IS 8880-2, "Information technology - Telecommunications and information exchange between systems - Protocol combinations to provide and support the OSI Network Service", Part 2: Provision and support of the connection-mode Network Service, ISO, 1992.

[11] IS 8880-3, "Information technology - Telecommunications and information exchange between systems - Protocol combinations to provide and support the OSI network service", Part 3: Provision and support of the connectionless-mode Network Service, ISO, 1990.

[12] IS 8473, "Information processing systems - Data communications - Protocol for providing the connectionless-mode network service, ISO, 1988.

[13] DAM 8473, "Amendment 5: Provision of the underlying service for operation over ISDN circuit-switched B-channel", ISO, 1993.

14] DAM 8473, "Addition of an ECHO function to ISO 8473", Part: 1, ISO.

[15] IS 8473/AD3, "Addendum 3: Provision of the underlying service assumed by ISO 8473 over subnetworks which provide the OSI data link service," ISO, 1989.

[16] DIS 8473-1, "Information technology - Protocol for providing the the connectionless-mode network service: Protocol specification", ISO, 1993.

[17] TR 9577, "Information technology - Telecommunications and information exchange between systems - Protocol identification in the OSI network layer", ISO, 1990.

[18] DTR 9577, "Information technology - Telecommunications and information exchange between systems - Protocol identification in the OSI network layer", ISO, 1993.

[19] TR 9575, "Information technology - Telecommunications and information exchange between systems - OSI Routeing Framework", ISO, 1990.

[20] IS 9542, "Information processing systems - Telecommunications and information exchange between systems - End system to Intermediate system routeing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473)", ISO, 1988.

[21] DAM 9542, "Amendment 1: Dynamic discovery of OSI NSAP addresses by end systems", ISO, 1992.

[22] IS 10030, "Information technology - Telecommunications and information exchange between systems - End System Routeing Information Exchange Protocol for use in conjunction with ISO 8878", ISO, 1990.

[23] DAM 10030, "Amendment 1: Dynamic discovery of OSI NSAP addresses by end systems", ISO, 1992.

[24] DAM 10030, "Amendment 2: PICS", ISO, 1992.

[25] DAM10030, "Amendment 3: Specifications of IS-SNARE interactions", ISO, 1992.

[26] IS 10589, "Information technology - Telecommunications and information exchange between systems - Intermediate system to intermediate system intra-domain routeing exchange protocol for use in conjunction with the protocol for providing CLNS (ISO 8473)", ISO, 1992.

[27] DIS 10028, "Information technology - Telecommunications and information exchange between systems - Definition of the relaying functions of a network layer intermediate system - Connection-mode network service", ISO, 1993.

[28] DTR 13531, "Information technology - Telecommunications and information exchange between systems - Definition of the relaying functions of a network layer intermediate system - Connectionless-mode network service, ISO, 1993.

[29] DIS 10747, "Information technology - Telecommunications and information exchange between systems - Protocol for exchange of inter-domain routeing information among intermediate systems to support forwarding of ISO 8473 PDUs", ISO, 1992.

[30] IS 8208, "Information processing systems - Data communication - X.25 Packet Level Protocol for Data Terminal Equipment", ISO, 1990.

[31] IS 8208/AM1, "Amendment 1: Alternative Logical Channel Identifier assignment", ISO, 1990.

[32] IS 8208/AM3, "Amendment 3: Conformance Requirements", ISO, 1990.

[33] DIS 8208, "Information technology - Data communications - X.25 Packet Level Protocol for Data Terminal Equipment", ISO, 1993.

[34] IS 10588, "Information technology - Use of X.25 Packet Layer Protocol in conjunction with X.21/X.21bis to provide the OSI connection-mode network service", ISO, 1993.

[35] IS 8878, "Information technology - Telecommunications and information exchange between systems - Use of X.25 to provide the OSI Connection-mode Network Service", ISO, 1992.

[36] IS 8878/AD1, "Addendum 1: Priority", ISO, 1990.

[37] IS 8878/AD2, "Addendum 2: Use of an X.25 PVC to provide the OSI CONS", ISO.

[38] IS 8878/AM3, "Amendment 3: Conformance, ISO, 1991.

[39] IS 8881, "Information processing systems - Data communications -"Use of the X.25 packet level protocol in local area networks", ISO, 1989.

[40] IS 9574, "Information processing systems - Data communications - Provision of the OSI connection-mode network service by packet mode terminal equipment connected to an Integrated Services Digital Network (ISDN)", ISO, 1989.

[41] IS 10732, "Information technology - Use of X.25 Packet Layer Protocol to provide the OSI connection-mode Network Service over the telephone network", ISO, 1993.

[42] DIS 11577, "Information technology - Telecommunications and information exchange between systems - Network layer security protocol", ISO, 1993.

[43] F. Delpino, A. Ghiselli, "Schema dell'indirizzo ISO DCC NSAP per l'Italia", Documento di GARR-DECnet e Gruppo di lavoro CLNP, INFN CNAF, Bologna, 1994.

18

LE ARCHITETTURE DI RETE SNA, APPN, HPR/APPN+ E BBNS

18.1 INTRODUZIONE

La IBM Corporation è sempre stata uno degli attori principali nel mondo delle reti di calcolatori. La sua principale architettura di rete è SNA (*System Network Architecture*) la cui introduzione è iniziata nel 1974 ed è terminata nel 1978.

SNA è una architettura di rete proprietaria, anche se realizzata da altri costruttori di calcolatori e apparati di rete. SNA è una architettura pensata per sistemi informativi basati su mainframe che devono interconnettere un grandissimo numero di terminali distribuiti sul territorio.

Questa struttura, concepita con uno o più mainframe al centro, ha reso meno interessante SNA per le applicazioni odierne, concepite per operare in modalità client-server, tipicamente tra elaboratori più piccoli (mini e personal computer).

La risposta di IBM a queste nuove necessità è stata la definizione di una strategia di networking più ampia, mostrata in figura 18.1.

La nuova strategia prevede di continuare il supporto di SNA, di sviluppare una rete nuova (APPN) e di usare standard affermati. Inoltre essa evidenzia che:

- le interfacce di programmazione (API) devono essere indipendenti dal tipo di trasporto offerto dalla rete;
- i protocolli di trasporto devono essere indipendenti dal livello Data Link ed avere una semantica comune.

IBM ha definito una semantica comune di trasporto multiprotocollo detta CTS (*Common Transport Semantic*). L'architettura CTS è realizzata, nei prodotti della famiglia MPTN (*Multi Protocol Transport Networking*) quali, ad esempio, IBM AnyNet, che consentono la scrittura di applicativi indipendenti dal trasporto.

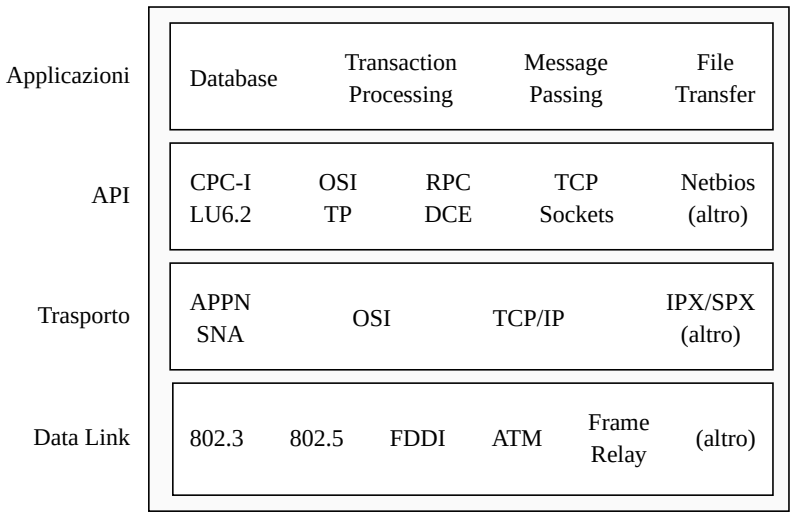


Fig. 18.1 - Networking blueprint di IBM.

Questa nuova strategia IBM ha già trovato una sua applicazione a vari livelli:

- a livello Data Link IBM ha iniziato a fornire supporto, oltre che per collegamenti proprietari quali il canale IBM e SDLC, anche per reti standard quali X.25, Token Ring, IEEE 802.3, FDDI, Frame Relay e ATM;
- a livello di trasporto è stato introdotto TCP/IP, vista la grande richiesta del mercato, ma gli sviluppi strategici puntano su APPN (*Advanced Peer to Peer Network*), una rete ad alte prestazioni sviluppata da IBM, sulla sua evoluzione HPR/APPN+, e su un ulteriore sviluppo verso le reti a larga banda detto BBNS (*Broad Band Network Service*);
- a livello di API la scelta preferenziale IBM è APPC (*Advanced Program-to-Programm Communication*) un servizio di comunicazione noto anche con la sigla LU 6.2 e normalmente utilizzato tramite la CPI-C (*Common Programming Interface for Communication*), una interfaccia disponibile su varie piattaforme.

La figura 18.2 mostra in modo comparato il modello di riferimento OSI, e le architetture di rete TCP/IP, SNA e APPN. Con riferimento a tale figura occorre evidenziare che anche in APPN, come in SNA, esistono funzioni di data flow control e di management service. Le differenze principali tra queste due architetture risiedono nel modo di decidere gli instradamenti e di fare il routing, e nella distribuzione delle funzioni di management. In SNA tali funzionalità sono concentrate, mentre in APPN sono distribuite.

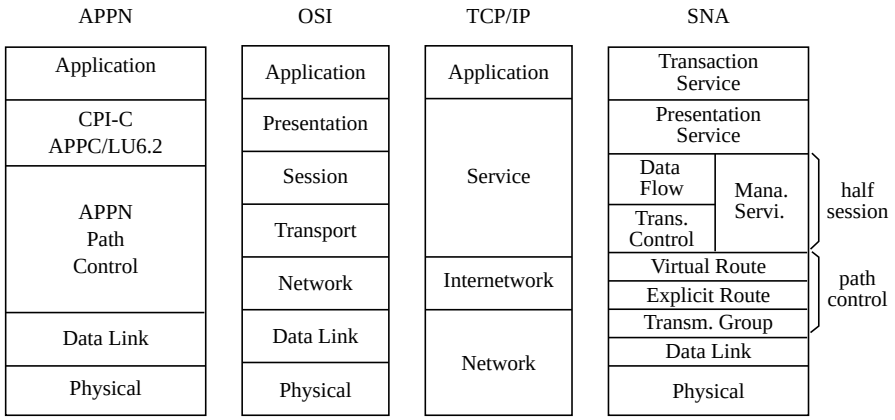


Fig. 18.2 - Architetture di rete.

18.2 LA RETE SNA

L'architettura di rete SNA è stata concepita da IBM per facilitare la condivisione delle risorse e, in particolare, per permettere ad ogni terminale di accedere ad ogni applicativo, per permettere un migliore utilizzo delle linee (con SNA viene introdotto il protocollo SDLC), per permettere di raggruppare una o più linee in una struttura detta *transmission group* o *trunk*, per consentire la comunicazione tra applicativi diversi, per decentrare le funzioni di rete all'esterno dell'host, per garantire l'indipendenza della rete dai collegamenti fisici e dai dispositivi e per avere una struttura hardware e software gerarchica.

Poiché molti nodi di rete IBM sono in grado di operare attualmente sia con SNA sia con APPN, quando si vuole fare esplicitamente riferimento alle funzionalità originali di SNA si usa la terminologia *hierarchical SNA* o *subarea SNA*. Il paragrafo 18.2 è dedicato alla descrizione di subarea SNA.

18.2.1 Il livello Fisico e Data Link

A livello Fisico e Data Link (figura 18.2) le reti SNA possono usare varie tecnologie trasmissive. Le prime due ad essere introdotte sono state il canale (si veda il paragrafo 18.2.2) e le linee trasmissive punto-punto e punto-multipunto con il protocollo SDLC (si veda il paragrafo 13.2).

A questi sono seguite le reti X.25, la rete locale Token Ring e più recentemente IEEE 802.3, FDDI, ATM, ISDN e Frame Relay.

A livello Data Link la rete SNA utilizza sempre protocolli connessi; ad esempio, sulle reti locali SNA usa un LLC di tipo 2.

18.2.2 Il canale

Il canale è una struttura di comunicazione di lunghezza limitata, ad alte prestazioni, utilizzata per interconnetere le risorse di rete all'host. Esistono due tipi di canale:

- *Bus-and-Tag* è un canale parallelo (trasferisce un byte alla volta) in rame con prestazioni di circa 4 Mbyte/s e lunghezza massima di 120 m;
- *ESCON (Extended System CONnection)* è un canale seriale in fibra ottica che, rispetto al Bus-and-Tag, è in grado di coprire distanze maggiori (sino a 43 Km), con prestazioni circa 8 volte superiori.

18.2.3 Tipi di nodi

I nodi di una rete SNA possono essere di vario tipo (figura 18.3) e sono descritti nei paragrafi seguenti.

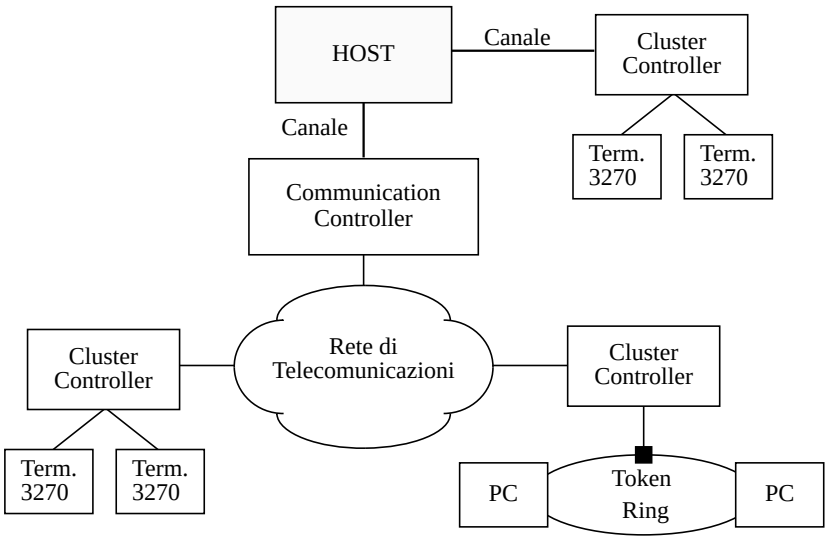


Fig. 18.3 - Componenti fisici di una rete SNA.

18.2.4 Host

Sono i nodi di rete che, oltre ad eseguire i programmi applicativi, realizzano funzioni di controllo sulla rete.

Le principali famiglie di host IBM sono:

- S/36 e S/38. Sistemi 36 e Sistemi 38 sono due architetture simili di minicomputer, ormai obsolete e sostituite dall'architettura AS/400.
- AS/400. Famiglia di host di medie prestazioni, compatibile con i precedenti S/36 e S/38.
- S/370. Architettura IBM del passato, include modelli che hanno avuto una larga diffusione quali la linea ad alte prestazioni 3090 e la linea a basse prestazioni 9370.
- 43XX. Famiglia di host di medie prestazioni, compatibile con la famiglia S/370.
- S/390. Architettura attuale, annunciata nel 1991, include i modelli della famiglia ES/9000.

18.2.5 Communication controller

I *communication controller* sono nodi dedicati al controllo delle linee di comunicazione ed in grado di fornire servizi di instradamento (routing).

Detti anche FEP (*Front End Processor*) sono normalmente connessi agli host tramite canale. Possono essere collegati in modalità punto-punto o punto-multipunto con altri FEP e possono collegare reti locali. Ammettono connessioni "a valle" con i cluster controller e altri nodi periferici.

Il modello attuale si chiama 3745, mentre modelli del passato sono stati il 3725, il 3720 e il 3705.

Per questa ragione vengono anche indicati collettivamente con la sigla 37XX.

I communication controller utilizzano un software di rete detto NCP (*Network Control Program*). A volte sul communication controller possono essere presenti anche altri programmi quali NPSI (*Network Packet Switched Interface*) per la connessione a reti X.25.

Dalla versione di NCP 6.2 in poi, i FEP sono anche nodi APPN e quindi forniscono supporto contemporaneamente ad entrambe le architetture di rete.

18.2.6 Cluster controller

I *cluster controller* sono concentratori in grado di connettere terminali, stampanti ed altri dispositivi di I/O. Possono essere collegati a canale, ad una LAN, oppure remotizzati tramite una linea punto-punto o punto-multipunto. In quest'ultimo caso sono connessi ad un FEP.

Il cluster controller gestisce le comunicazione per le risorse ad esso connesse (terminali, stampanti, ecc.).

Il modello attualmente utilizzato si chiama IBM 3174 (enterprise controller); un modello precedente era il 3274. Per questa ragione i cluster controller vengono anche indicati collettivamente con la sigla 3X74.

18.2.7 Interconnect controller

Sono dispositivi collegati a canale, progettati per connettere un host a varie reti locali (Ethernet, Token Ring e FDDI). Il modello attuale è l'IBM 3172 (interconnect controller).

18.2.8 Multiprotocol router

IBM ha introdotto sul mercato dei multi-protocol router detti IBM 6611 (network processor router) che sono stati pensati per APPN, ma che possono essere un valido veicolo di interconnessione di reti TCP/IP e SNA.

In particolare, essi sono in grado di operare come source routing bridge tra reti token-ring o come transparent bridge tra reti Ethernet, e di realizzare una modalità di interconnessione di LAN remote SNA e Netbios su trasporto TCP/IP, detta DLS (*Data Link Switching*) e specificata nello RFC 1434.

18.2.9 Terminali

Le due famiglie principali di terminali sono:

- *IBM 3270*. Una famiglia di terminali video, stampanti e controllori comunemente usata nelle reti SNA con elaboratori delle famiglie S/370, 43XX e S/390. I terminali 3270 si collegano al cluster controller tramite un cavo coassiale, con un collegamento di tipo punto-punto su cui opera un protocollo sincrono.

- *IBM 5250*. Una famiglia di terminali video, stampanti e controllori comunemente usata nei minicomputer IBM quali i Sistemi 36 (S/36), i Sistemi 38 (S/38) e gli AS/400. I terminali 5250 si collegano tramite un cavo biassiale, con un collegamento di tipo punto-punto o punto-multipunto su cui opera un protocollo sincrono.

Esempi di terminali 3270 sono il 3278 e il 3279, anche se oggi è molto comune utilizzare un personal computer con scheda di emulazione 3270.

18.2.10 NAU

Le NAU (*Network Addressable Unit*) sono le entità di rete indirizzabili che possono comunicare tramite la rete. Tutte le risorse di rete hanno un indirizzo, ma non tutte sono NAU. Ad esempio, una linea ha un indirizzo, ma non è una NAU in quanto non è mittente o destinataria di trasmissioni.

Esistono tre tipi di NAU:

- *LU: Logical Unit*;
- *PU: Physical Unit*;
- *SSCP: Session Service Control Point*.

La relazione tra le NAU, la rete e gli utenti finali è rappresentata in figura 18.4.

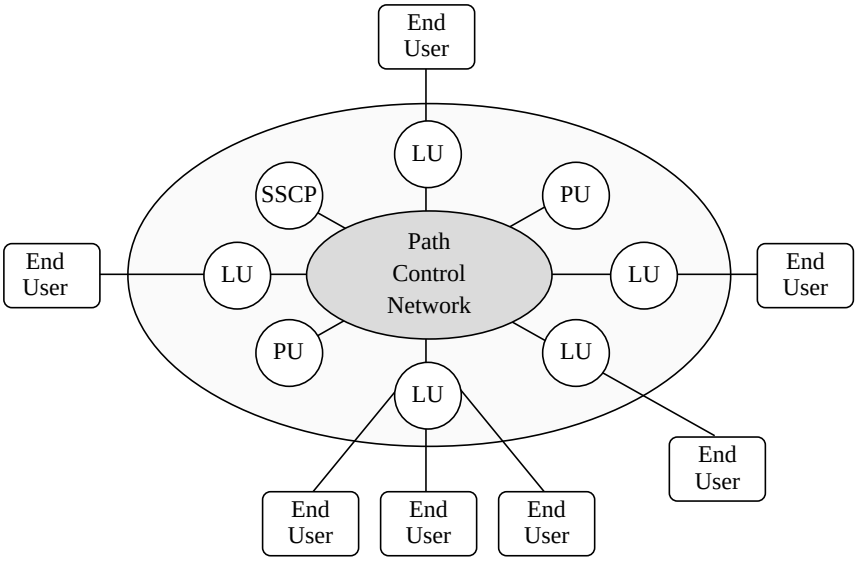


Fig. 18.4 - Componenti logici di una rete SNA.

18.2.11 SSCP

Lo SSCP è un insieme di funzionalità di configurazione, controllo e gestione delle risorse di rete, implementato nel software VTAM (*Virtual Telecommunications Access Method*). Ogni SSCP gestisce un dominio e mantiene tabelle di nodi, linee, nomi, indirizzi e altre risorse appartenenti al dominio. Esiste una relazione biunivoca tra un SSCP e un dominio.

Lo SSCP attiva e disattiva la rete, stabilisce e termina la comunicazione tra tutte le risorse di rete.

Il VTAM è il software di rete sugli host S/370 e S/390. Include al suo interno le funzionalità di SSCP e di PU, oltre al supporto per le LU degli applicativi.

Nel 1987 IBM ha rilasciato la versione 4 release 1 (V4R1) del VTAM che include anche le funzionalità di nodo APPN CP e ha tipo di nodo 2.1.

18.2.12 PU

La PU (*Physical Unit*) è la NAU che serve per la gestione di un nodo di rete SNA ed in particolare per il downline loading del software, per l'upline dumping della memoria, per l'attivazione e deattivazione dei collegamenti, ecc.

La PU, oltre a gestire il nodo su cui risiede, gestisce anche risorse connesse al nodo che siano sprovviste di una PU (ad esempio, i terminali). Le PU sono presenti sugli host, sui communication controller e sui cluster controller. Anche gli interconnect controller hanno una PU per scopi di gestione.

La PU lavora in connessione con lo SSCP.

18.2.13 End user

Gli utenti finali della rete (*end user*) sono i programmi applicativi, i terminali d'utente e i dispositivi di I/O. SNA permette di stabilire connessioni tra:

- programma applicativo e terminale d'utente;
- programma applicativo e programma applicativo;
- programma applicativo e dispositivo di I/O.

La comunicazione viene stabilita tramite la *path control network* (figura 18.4) specificando l'indirizzo delle LU.

18.2.14 LU

Ogni utente finale accede alla rete SNA tramite le LU (*Logical Unit*). Le LU sono realizzate dal software VTAM, dall'APPC e da altri software/firmware di comunicazione. Le LU sono divise in vari tipi:

- LU 0 utilizzate particolarmente in ambiente finanziario per semplici scambi di dati;
- LU 1 utilizzate per i dispositivi batch;
- LU 2 utilizzate dai terminali 3270;
- LU 3 utilizzate da certi tipi di stampanti;
- LU 4 utilizzate dai terminali 5250;
- LU 6 utilizzate per comunicazione tra programmi (particolarmente importante la LU 6.2 o APPC);
- LU 7 utilizzate dai terminali 5250.

Le LU di tipo 1, 2, 3, 4, 7 sono anche dette DLU (*Dependent LU*) in quanto dipendono dallo SSCP e quindi dall'host per l'attivazione e la disattivazione delle sessioni. Le LU di tipo 6.2 sono dette invece *independent LU* in quanto possono stabilire sessioni tra loro senza necessariamente richiedere la presenza di un host. Questa classificazione è particolarmente importante per la migrazione ad APPN.

Le LU sono controllate dalla PU del dispositivo su cui risiedono. Le LU dei programmi applicativi risiedono sull'host che ospita il programma, mentre quelle dei terminali e dei dispositivi di I/O risiedono sui communication e sui cluster controller.

18.2.15 LU 6.2 - APPC

Il servizio APPC permette ad applicativi di condurre una conversazione paritetica (*peer-to-peer*) tramite una sessione half-duplex o full-duplex. Gli end node possono gestire più sessioni con più applicativi diversi o più sessioni parallele con lo stesso applicativo.

Quando è stata stabilita una sessione tra due nodi, essa può ospitare più conversazioni, consentendo un risparmio di risorse sui nodi e sui collegamenti.

APPC offre alle applicazioni un ricco insieme di servizi aggiuntivi quali la sicurezza, la sincronizzazione, l'attivazione di processi e la gestione degli errori.

18.2.16 Subaree

Per facilitare il routing dei pacchetti, una rete SNA è divisa in partizioni chiamate subaree. La topologia interna di una subarea è un albero e quindi ammette un solo cammino tra due punti qualsiasi della subarea, mentre la topologia di interconnessione delle subaree può essere magliata a piacere.

Una subarea può contenere:

- un host e tutte le risorse ad esso connesse, con eccezione dei communication controller;
- un communication controller e tutte le risorse fisiche ad esso connesse, ad eccezione degli host e dei communication controller.

La figura 18.5 mostra una rete SNA con due subaree (SA03 e SA01).

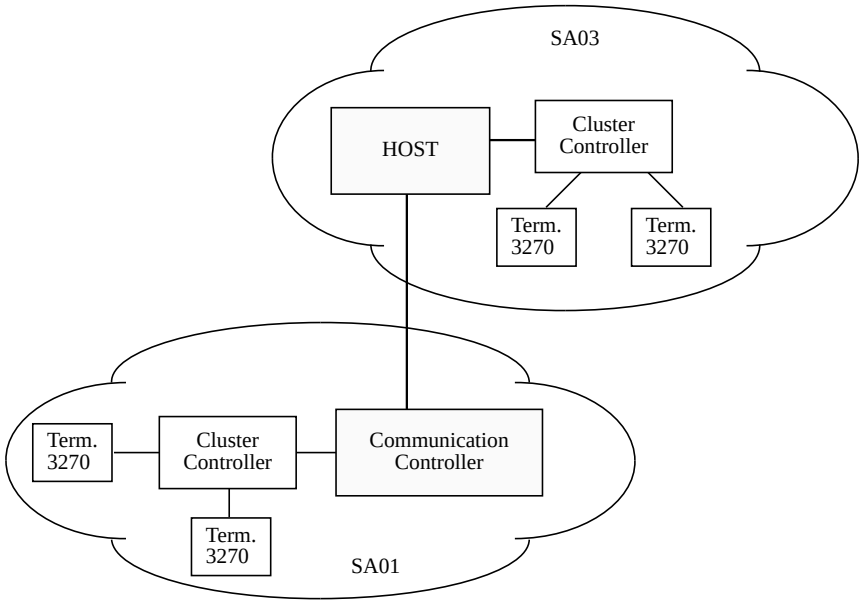


Fig. 18.5 - Subaree SNA.

Ogni subarea è identificata da un indirizzo numerico. Nell'esempio precedente l'host appartiene alla subarea con indirizzo 3, identificata dalla sigla SA03. L'indirizzo di subarea fa parte dell'indirizzo di ciascuna risorsa di rete.

18.2.17 Tipi di nodo

I nodi di rete SNA si dividono in quattro tipi:

- tipo 5: gli host;
- tipo 4: i communication controller;
- tipo 2: i cluster controller aventi al massimo 255 LU;
- tipo 1: i cluster controller con una sola LU.

Ad ogni tipo di nodo corrisponde un tipo di PU: PU_T5 per i nodi di tipo 5, PU_T4 per i nodi di tipo 4, ecc. La figura 18.6 mostra i vari tipi di nodo e le NAU in essi contenute.

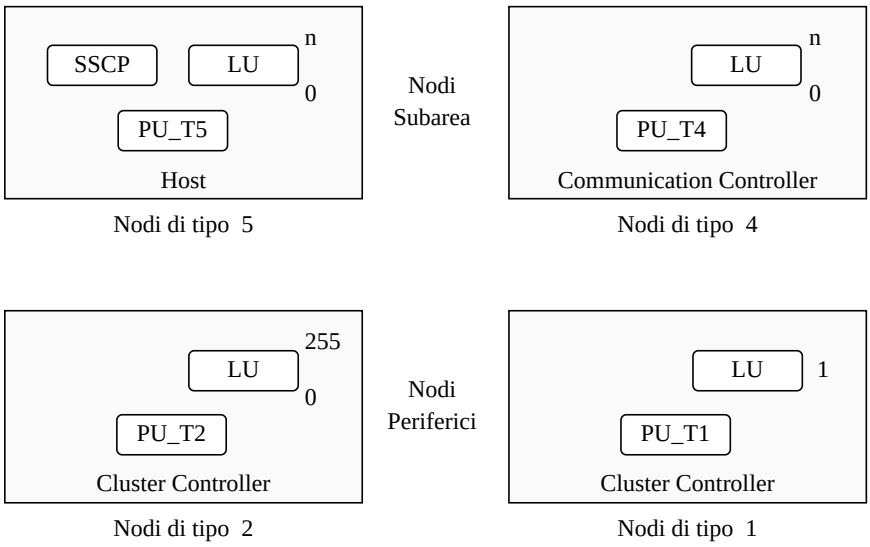


Fig. 18.6 - Tipi di nodo.

Si noti che i nodi vengono suddivisi in due gruppi:

- nodi subarea: tipo 5 e tipo 4;
- nodi periferici: tipo 2 e tipo 1.

I nodi subarea (host e communication controller) sono così chiamati perché sono a capo di una subarea e gestiscono i collegamenti con le altre subaree (*cross-subarea link*), risolvendo le relative problematiche di instradamento. I nodi periferici (cluster controller) gestiscono solo connessioni all'interno della subarea. Un esempio di connessione di nodi dei due tipi è mostrato in figura 18.7.

Due subaree connesse da uno o più cross-subarea link sono dette adiacenti.

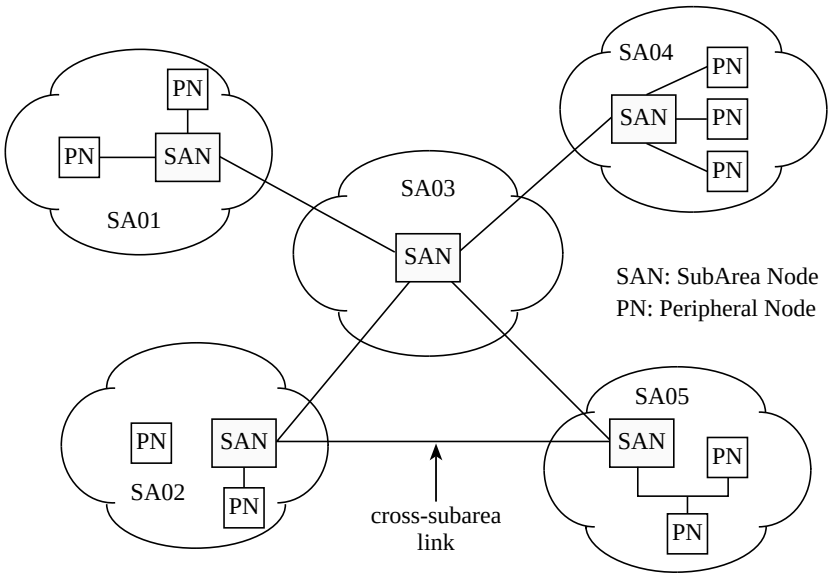


Fig. 18.7 - Nodi SNA: subarea e periferici.

18.2.18 Domini

Una rete SNA è suddivisa a livello logico in domini. Un dominio è una partizione di rete gestita da un SSCP e quindi ci sono tanti domini quanti sono gli host. Un dominio comprende una o più subaree. Le subaree associate agli host appartengono ai domini degli host, mentre quelle associate ai communication controller possono appartenere a uno o più domini. In quest'ultimo caso si dicono sotto controllo condiviso *(shared control).*

La figura 18.8 mostra una rete SNA con 3 subaree e 2 domini.

La subarea SA01 appartiene al dominio dell'host A01M, mentre la subarea SA03 appartiene al dominio dell'host A03M. La subarea SA05 può appartenere ad entrambi i domini, ma appartiene in un dato istante al dominio dello SSCP che ne ha attivato le risorse e ne ha il controllo.

Alcune risorse possono essere condivise in modo concorrente, cioè due o più SSCP possono contemporaneamente attivare e controllare la stessa risorsa. Questo è il caso dei communication controller. Altre risorse possono essere condivise serialmente, cioè se un SSCP non controlla più la risorsa, questa passa sotto il controllo di un altro SSCP. I cluster controller sono esempi di risorse che possono essere condivise serialmente.

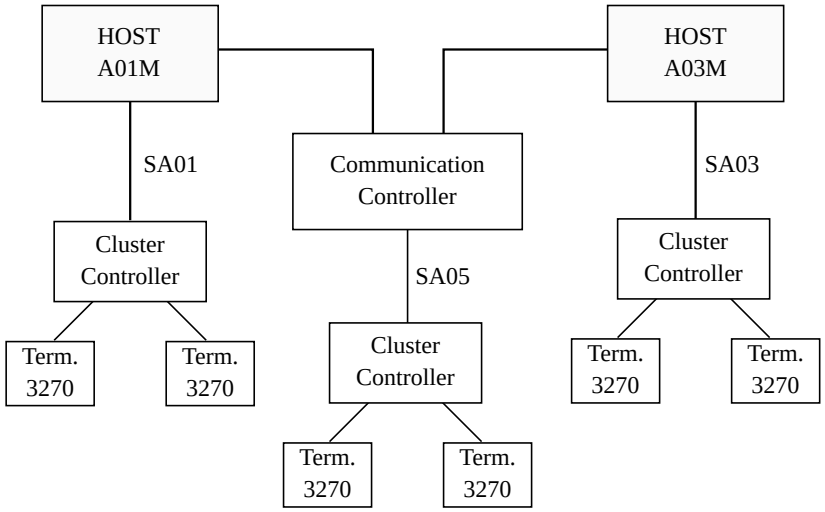


Fig. 18.8 - Domini.

18.2.19 Sessioni

Le NAU interagiscono tra loro tramite le sessioni. Una sessione è una relazione temporanea tra due NAU. Quando una sessione è stabilita (*bind* della sessione), le NAU concordano le caratteristiche della comunicazione, quali: full o half duplex, error recovery, data blocking, acknowledgement scheme, ecc..

La NAU che richiede il bind della sessione è detta primaria, quella che accetta il bind secondaria. La sessione è divisa in due parti ciascuna detta *half session*. Una half session risiede sulla primary NAU e l'altra sulla secondary NAU.

Si noti in figura 18.2 come le half session siano i livelli intermedi dell'architettura di rete SNA, collocandosi tra gli applicativi e il path control.

Ogni nodo di rete può contenere più NAU e ogni NAU più half session, come mostrato in figura 18.9.

Esistono vari tipi di sessione:

- *SSCP-PU*. È utilizzata dallo SSCP per controllare le PU delle risorse appartenenti al suo dominio. Tramite questo tipo di sessione lo SSCP può attivare, disattivare e raccogliere informazioni sulle risorse, mentre la PU può comunicare allo SSCP eventuali errori.
- *LU-LU*. È l'unico tipo di sessione che fornisce i servizi di rete agli utenti finali. Tramite una sessione LU-LU un terminale comunica con un applicativo o due

applicativi comunicano tra loro. La LU primaria deve effettuare una richiesta di bind allo SSCP, che la inoltra alla LU secondaria che può accettarla o no.

- *SSCP-LU*. Tutte le LU che non sono impegnate in sessioni LU-LU devono essere in sessione con lo SSCP che le controlla. Tramite questo tipo di sessione una LU può chiedere allo SSCP il bind di una sessione LU-LU.
- *SSCP-SSCP*. Sono sessioni con cui gli SSCP si scambiano informazioni riguardanti le risorse appartenenti ai relativi domini.

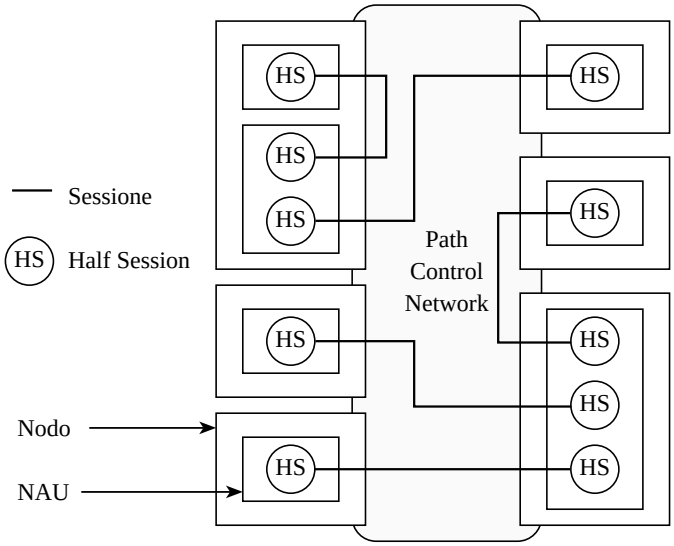


Fig. 18.9 - Sessioni tra NAU.

18.2.20 Bind e unbind

Il bind di una sessione LU-LU avviene se entrambe le LU sono libere (in sessione con lo SSCP). Una delle due LU chiede allo SSCP il bind della sessione, lo SSCP verifica la disponibilità dell'altra LU e, se positiva, stabilisce la sessione LU-LU. Le due LU a questo punto dialogano direttamente usando un cammino, sulla path control network, fisso e determinato in fase di bind. Tale cammino può passare oppure no per l'host, ma comunque non coinvolge lo SSCP. Una sessione LU-LU dura sino a quando le due LU hanno dati da scambiarsi, tipicamente dal logon al logoff. La sessione LU-LU viene terminata da una richiesta di *unbind* effettuata da una delle due LU. Le sessioni LU-SSCP continuano a rimanere attive per le funzioni di gestione delle LU.

18.2.21 Cross-domain

Il termine cross-domain indica che una risorsa è in un altro dominio o anche una connessione tra due domini. Un esempio tipico è una sessione cross-domain tra due LU: una LU appartenente ad un dominio vuole scambiare dati con una LU appartenente ad un altro dominio.

Il bind della sessione in questo caso è più complesso e richiede la presenza di un *cross-domain resource manager*, che è parte integrante dello SSCP. I cross-domain resource manager si scambiano i dati tramite sessioni SSCP-SSCP.

18.2.22 La path control

La componente path control di SNA si occupa di instradare i messaggi sulla rete. Essa fornisce un servizio di tipo connesso.

L'instradamento di una sessione viene deciso in fase di bind della sessione e non può essere modificato. Se un elemento lungo il cammino (path) della sessione ha dei problemi, la sessione cade e può essere riattivata se esiste un cammino alternativo.

SNA usa un algoritmo di instradamento statico basato su tabelle di instradamento con più alternative. Le tabelle sono scritte manualmente sui vari nodi della rete. Poiché il compito è particolarmente gravoso, esistono strumenti di ausilio alla scrittura delle tabelle SNA, quali NETDA (*NETwork Design Aid*) che operano però fuori linea.

Le problematiche di instradamento sono in parte differenziate all'interno di una subarea o tra subaree diverse. Questo è anche riflesso dalla struttura del pacchetto di path control (*Transmission Header*) che nel primo caso è più semplice ed è detto FID2 (*Format IDentifier 2*), mentre nel secondo caso caso è più complessa (FID4). Un esempio di pacchetto FID2 su LAN è riportato in appendice B, paragrafo B.2.1.

Il path control è suddiviso ulteriormente in tre sottolivelli (figura 18.2): Virtual Route, Explicit Route e Transmission Group.

18.2.23 Virtual Route

Le *Virtual Route* (VR) sono cammini alternativi tra subaree, anche non adiacenti. SNA ammette che tra due subaree siano specificate sino a 8 VR, denominate VR0, VR1, ..., VR7.

Quando SNA deve fare il bind di una sessione tra due NAU appartenenti a subaree diverse, ne determina l'instradamento provando ordinatamente le VR dalla 0 alla 7. La

prima che risulta essere percorribile, diviene l'instradamento per la sessione.

Se la sessione cade e viene fatta ripartire, SNA riprova le VR nello stesso ordine.

18.2.24 Explicit Route

Le *Explicit Route* (ER) sono otto come le VR e sono chiamate ER0, ER1, ..., ER7. Una ER è una porzione del cammino che connette due subaree adiacenti. Una VR tra due NAU si può attivare quanto tutte le ER sul cammino sono attive.

18.2.25 Transmission Group

I cross-subarea link tra due subaree adiacenti sono raggruppati in uno o più gruppi detti *Transmission Group* (TG). Un TG può consistere in una sola linea o in più linee parallele, normalmente con caratteristiche fisiche simili (ad esempio la velocità).

La disponibilità dei TG era molto importante nel passato, quando non erano disponibili canali trasmissivi geografici veloci e l'unica possibiltà era quella di costruirli raggruppando canali più lenti in un TG.

Se una linea che fa parte di un TG ha un guasto ed esistono altre linee del TG attive, il TG continua ad operare con prestazioni ridotte.

Il concetto di TG rimane comunque importante anche oggi, poiché l'instradamento di un messaggio da una subarea all'altra avviene specificando il numero del TG.

18.2.26 Transmission priority

Al traffico è associata una priorità di trasmissione (*transmission priority*). SNA ammette tre priorità identificate con i numeri 0, 1, e 2; 0 è la priorità minore, 2 quella maggiore. La priorità serve per ordinare i pacchetti che sono accodati su un link in attesa di trasmissione.

18.2.27 Class Of Service

Le classi di servizio (COS: *Class Of Service*) sono concetti logici che raggruppano al loro interno la priorità di trasmissione e le VR.

Su una rete SNA è possibile definire più classi di servizio, ad esempio batch, interattivo, network, ecc. Queste classi di servizio specificano traffico a priorità diversa e che probabilmente deve seguire delle VR diverse.

La classe di servizio viene specificata in fase di bind della sessione e determina la VR scelta. La priorità associata viene invece usata in fase di trasmissione.

La tabella 18.1 mostra un esempio di tabella COS. Tale esempio indica che, se è richiesto un servizio INTERACT, si devono provare in ordine le VR da 0 a 6 con transmission priority uguale a 1.

COS Name	VR=(Virtual Route Number, Transmission Priority)
ISTVTCOS	VR=((0,2),(1,2),(2,2),(3,2),(4,2),(5,2),(6,2))
NETOPER	VR=((0,1),(1,1),(2,1),(3,1),(4,1),(5,1),(6,1))
INTERACT	VR=((0,1),(1,1),(2,1),(3,1),(4,1),(5,1),(6,1))
BATCH	VR=((0,0),(1,0),(2,0),(3,0),(4,0),(5,0),(6,0))

Tab. 18.1 - Esempio di tabella COS.

La consultazione della tabella COS che risiede sullo SSCP determina in quale ordine provare le VR.

18.2.28 Scelta dell'instradamento

Una NAU in una subarea chiede di stabilire una connessione con una NAU in un'altra subarea (ad esempio, SA04) e con un certo COS name (ad esempio, INTERACT).

1. Si consulta la entry INTERACT della COS table e si decide la prima VR da provare (ad esempio, VR0).
2. Con VR0 e SA04 si consulta la tabella sullo SSCP che indica quale ER usare (ad esempio, ER6).
3. Con ER6 si consulta un'ulteriore tabella che indica a quale subarea inviare il messaggio e quale TG usare (ad esempio, SA02 e TG4).
4. Se la SA02 è raggiungibile tramite il TG4 ci si "sposta" su SA02 e si ripete da 2. sino a quando o si giunge all'area di destinazione, o si fallisce (perché un TG o un nodo di subarea non sono attivi).

5. Se si fallisce, si torna a 1. e si prova la VR successiva.
6. La prima VR che consente di stabilire un cammino completo tra mittente e destinatario viene assegnata alla sessione ed utilizzata per l'instradamento di tutti i pacchetti relativi alla sessione stessa. La priorità di trasmissione usata è quella associata alla VR nella tabella COS e si utilizza, dopo che la VR è stata creata, per ordinare i pacchetti da trasmettere ad ogni attraversamento di un TG.

   Se nessuna VR ha successo, si dichiara la destinazione non raggiungibile.

18.3 LA RETE APPN

18.3.1 Introduzione

APPN è *l'Advanced Peer-to-Peer Networking*, una estensione di SNA annunciata nel 1987 e attualmente disponibile sulla maggior parte delle piattaforme IBM. APPN nasce come architettura di rete proprietaria, ma viene messa da IBM nel dominio pubblico per invogliare terze parti a sviluppare prodotti APPN.

La figura 18.10 mostra le fasi evolutive da SNA verso BBNS. APPN rappresenta la terza fase dopo Subarea SNA e LEN (*Low Entry Network*).

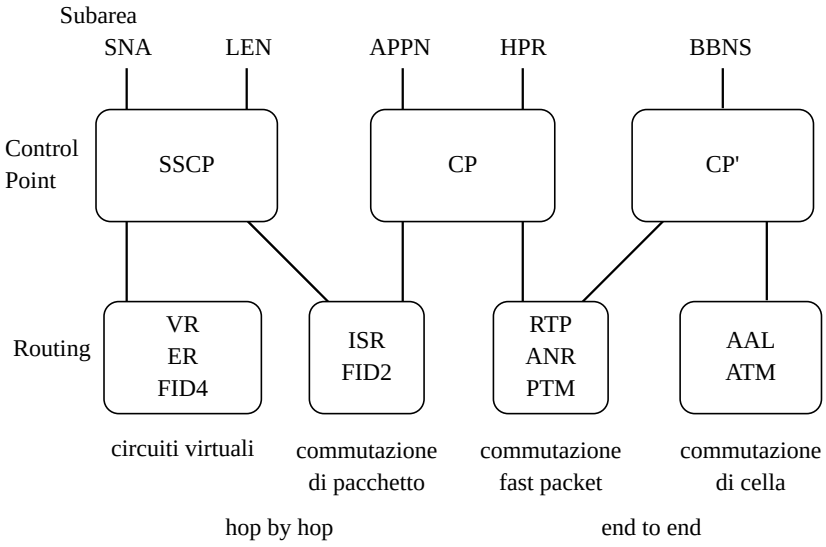


Fig. 18.10 - Evoluzione da SNA a BBNS.

La versione classica di SNA (subarea SNA) basa il controllo e la gestione della rete, e dei relativi instradamenti, sulla presenza dello SSCP. Il routing tra le subaree usa i meccanismi di Virtual Route e Explicit Route descritti precedentemente.

All'inizio degli anni '80 l'IBM ha introdotto il concetto di LEN (*Low Entry Network*) sui suoi minicomputer, per permettere ad applicativi sviluppati usando APPC di comunicare tra loro senza richiedere la presenza di uno SSCP. I nodi LEN sono in grado di instradare messaggi solo a nodi adiacenti (connessi alla stessa rete locale), ma le definizioni di rete e di sistema richieste sono poche e perciò i nodi LEN sono facili da installare ed usare.

I nodi LEN continuano a basarsi su un SCCP quando devono comunicare con un calcolatore non adiacente (più distante di un hop). I nodi LEN usano un protocollo basato sul FID2, precedentemente usato per il routing all'interno di una subarea (tra cluster e communication controller).

Nel 1986 la IBM ha introdotto APPN, che continua a basarsi sui pacchetti FID2, ma aggiunge capacità di instradamento. In particolare vengono introdotti gli APPN EN (*End Node*) e gli APPN NN (*Network Node*). Gli APPN NN contengono un CP (*Control Point*) che realizza le funzionalità di gestione, di directory service e di controllo simili a quelle degli SSCP. Con APPN non è più richiesta la compilazione di complesse tabelle di instradamento in quanto queste vengono compilate automaticamente da appositi algoritmi.

APPN ha un livello Network (ISR: *Intermediate Session Routing*) connesso e l'instradamento è stabilito in fase di bind della sessione e non può essere cambiato.

Inizialmente APPN era in grado di trasportare solamente traffico generato dalle independent LU e cioè da APPC, ma nel 1994 è comparsa anche la possibilità di trasportare traffico generato dalle DLU (*Dependent LU*), quali i terminali 3270.

Nel 1994 IBM ha introdotto HPR (*High Performance Routing*) detta anche APPN+, che implementa un routing dinamico in grado di reinstradare una sessione senza farla cadere. Alla base di HPR c'è la disponibilità di canali di comunicazione veloci e con basso tasso di errore. Con tali canali viene a cadere la necessità di avere un livello Data Link connesso: ad esempio, sulle LAN si può adottare una trasmissione non connessa.

HPR utilizza una tecnica di tipo source routing e può convivere con ISR. HPR introduce anche una serie di importanti novità, a livello di trasporto, per aumentare l'efficienza della rete, quali algoritmi sofisticati per prevenire e gestire le congestioni della rete.

Infine IBM ha annunciato BBNS (*Broad Band Network Service*) un insieme di funzionalità aggiuntive ad APPN, pensate per operare su reti ATM (si veda il capitolo 19).

Le principali differenze tra questi tipi di reti IBM sono raccolte in tabella 18.2.

Generazione	Control Point	Routing	Packet Format
Subarea SNA	SSCP, PU 4,5	ER e VR	FID4
LEN	SSCP*, NT 2.1	Solo nodi adiacenti	FID2
APPN	APPN CP, NT 2.1	ISR	FID2
HPR	APPN CP, NT 2.1	RTP e ANR	PTM (FID5)
BBNS	BBNS CP	ATM o PTM	Diversi (es: ATM e PTM)

* Un nodo LEN non necessita dello SSCP per comunicare con i nodi adiacenti
NT: Node Type

Tab. 18.2 - Evoluzione da SNA a BBNS.

18.3.2 Il livello Data Link

APPN è stata progettata in modo da essere indipendente dal livello Data Link usato. Esistono versioni di APPN in grado di operare su linee asincrone e sincrone, ISDN, X.25, frame relay, SDLC, canale IBM, oltre che sulle principali reti locali (figura 18.11).

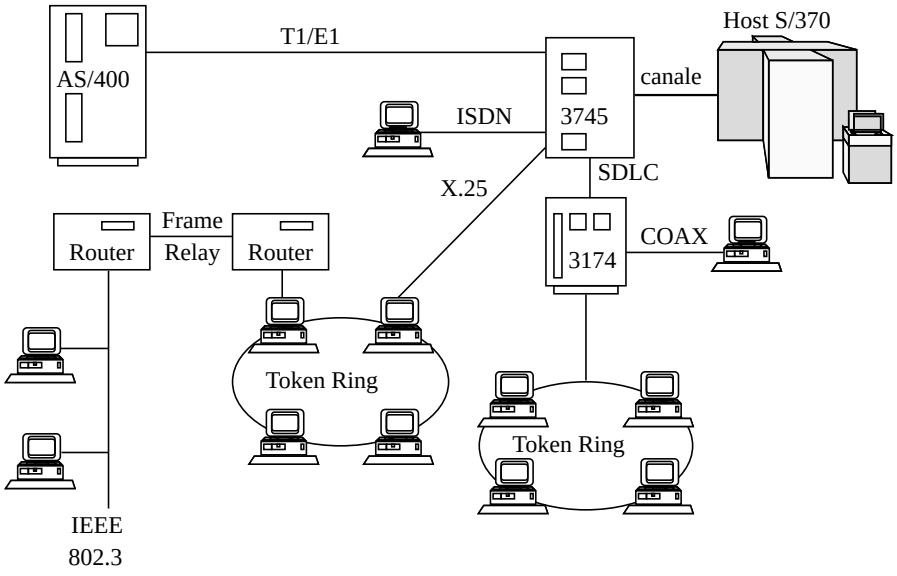


Fig. 18.11 - Esempio di rete APPN.

Teoricamente APPN può operare su linee da 1200 b/s sino a 45 Mb/s (T3). Per poter sfruttare le linee più veloci in modo efficiente occorre tuttavia utilizzare HPR o BBNS.

18.3.3 Topologie

APPN può operare su topologie miste magliate a piacere. I tipi di reti su cui APPN può essere utilizzato vanno dalla piccola LAN isolata alla grande rete aziendale con decine di migliaia di nodi.

18.3.4 APPN: nodi LEN

Un nodo APPN/LEN deve avere definiti localmente tutti gli indirizzi delle applicazioni con cui intende comunicare (figura 18.12a). Questo è scomodo, poco flessibile, difficile da mantenere aggiornato, ma riduce al minimo il software APPN che deve essere installato sul nodo.

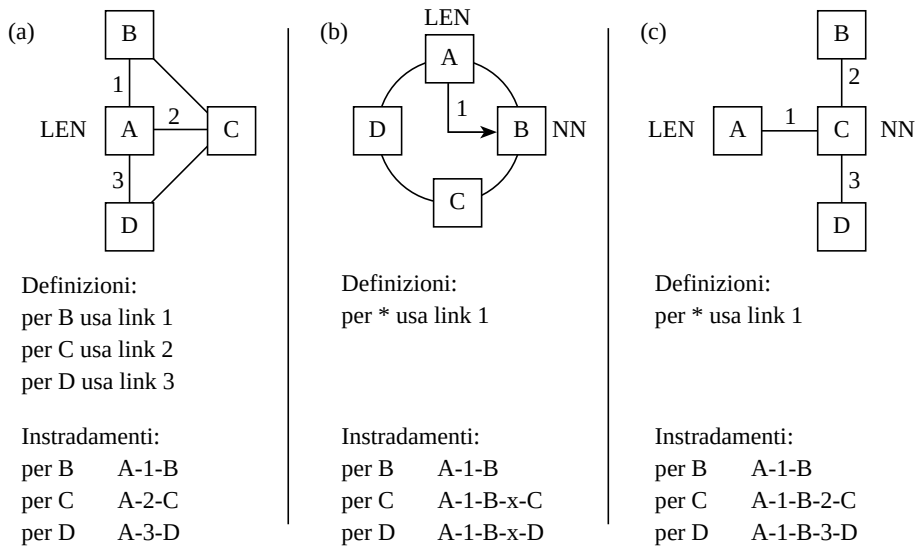


Fig. 18.12 - Routing dei nodi LEN.

Alternativamente, un nodo LEN può avere un'unica definizione che specifica il suo default NN. In questo secondo caso il nodo LEN invia tutto il traffico al suo default NN ignorando la possibilità di raggiungere direttamente alcune applicazioni. Questo può risultare una grave disottimizzazione se il traffico è destinato, ad esempio, ad un EN collegato alla stessa LAN (figura 18.12b), ma può risultare assolutamente idoneo nel caso di un PC remoto che si connette ad un NN tramite un collegamento commutato ISDN (figura 18.12c).

I nodi LEN sono spesso detti nodi pre-APPN. Un esempio di nodo pre-APPN è il PC con sistema operativo MS/DOS, per il quale non verrà prodotta una versione più sofisticata di APPN, a causa dei limiti intrinseci di MS/DOS.

18.3.5 APPN: End Node

Un EN (End Node) supera le limitazioni dei nodi LEN aggiungendo del software di rete per registrare su un NN le LU delle sue applicazioni, che vengono quindi automaticamente rese accessibili a tutta la rete, e per richiedere i servizi offerti dai NN.

Un EN continua ad essere relativamente semplice e poco costoso, in quanto delega la maggior parte delle funzionalità di rete al suo NN. In questo modo un EN ha più risorse libere per gli applicativi, ma partecipa comunque a pieno titolo ad una rete APPN. Un esempio di un EN APPN è un calcolatore AS/400 dotato di una singola connessione a LAN.

I nodi APPN non sono più suddivisi in quattro tipi come in SNA (tipo 1, 2, 4, 5), ma raggruppati nell'unico tipo NT 2.1 (*Node Type 2.1*). Si dice anche che un nodo APPN contiene una PU 2.1. La PU 2.1 coincide con il CP (*Control Point*) che non è presente sui nodi LEN, è presente con funzionalità ridotte sugli EN ed è completo sui NN.

18.3.6 APPN: Network Node

Un NN (Network Node) fornisce servizi di rete a nodi di tipo EN o LEN. Un NN può anche avere hardware specializzato per collegamenti locali o geografici (ad esempio, schede ISDN). I servizi offerti da un NN ad un EN sono principalmente quelli di directory service, di route selection service e di intermediate session routing.

Un NN può avere funzionalità di EN. I router IBM 6611 e i cluster controller 3174 sono esempi di NN che non hanno funzionalità di EN, mentre PC con OS/2, AS/400 e Risc 6000 sono esempi di NN che possono anche eseguire programmi applicativi e quindi essere allo stesso tempo EN e NN.

La figura 18.13 mostra l'architettura interna di un nodo APPN.

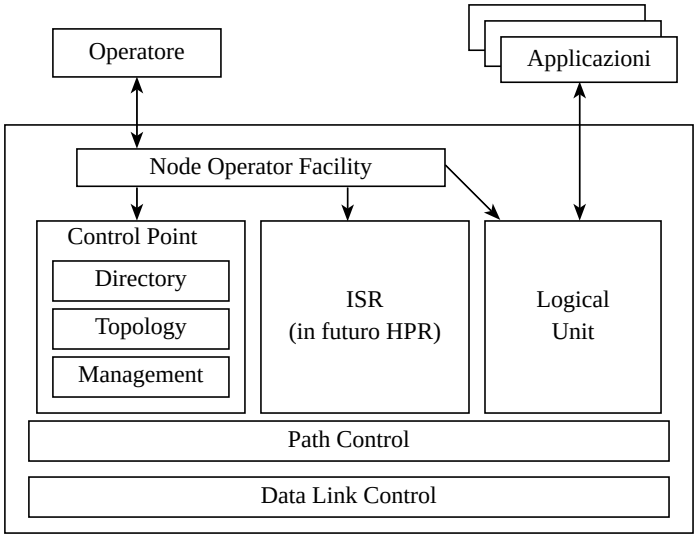


Fig. 18.13 - Architettura di un nodo APPN.

Le LU, il CP e tutte le altre componenti di un nodo APPN sono gestite da un operatore utilizzando la *node operator facility*. Essa permette di attivare/disattivare i link, definire/cancellare le LU ed effettuare altre operazioni di gestione o diagnosi.

Un NN contiene un *database topologico* che è replicato identico su ogni NN. I database topologici sono costruiti automaticamente tramite algoritmi di tipo link state packet (si veda il paragrafo 14.7). I database topologici contengono solo i NN e non gli EN o le loro LU. Questi due tipi di informazione (EN e LU) sono gestiti dal directory service.

Le variazioni di rete si propagano in modo incrementale e APPN pone grande attenzione nella minimizzazione del traffico dovuto a tali variazioni. L'unica occasione in cui un NN riceve un database topologico completo è quando viene connesso per la prima volta alla rete. Il database topologico può essere salvato su una memoria permanente e ricaricato da questa anche dopo lunghi periodi di inattività.

Ogni cinque giorni i NN riaffermano il loro database topologico con gli altri nodi. Se un'informazione non è riaffermata entro quindici giorni, viene cancellata dal database.

Inoltre una rete APPN può essere suddivisa in domini utilizzando dei *border node*.

Oltre al database topologico, un NN tiene traccia dei link ad esso collegati, degli EN che serve e delle risorse presenti sugli EN.

18.3.7 Servizio di directory

Il *servizio di directory* serve per localizzare un'applicazione sulla rete, cioè determinare qual è l'indirizzo del calcolatore che la contiene.

In particolare, il directory fornisce servizio alle LU e queste alle applicazioni. Quando un programma applicativo vuole comunicare con un altro programma applicativo chiede alla sua LU di localizzare la LU dell'altro programma (figura 18.14).

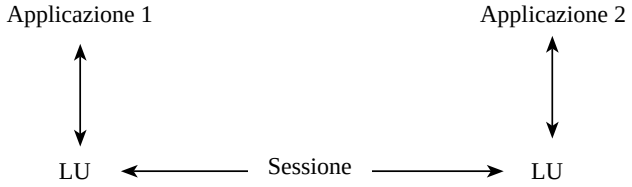


Fig. 18.14 - Relazione tra applicazioni.

Le due LU creano una sessione usando i servizi di routing di APPN e i due applicativi scambiano dati usando le LU.

Per localizzare le LU e altre risorse di rete, il servizio di directory di APPN effettua una ricerca a vari livelli:

- nel directory dell'EN;
- nel directory del NN, seguita da una ricerca diretta;
- in broadcast, effettuata dal NN;
- in un directory server centrale.

Questi vari livelli di ricerca minimizzano il lavoro di ricerca, confinando la ricerca stessa alla più piccola porzione di rete possibile.

Gli EN possono mantenere una breve lista di LU. Quando un'applicazione vuole localizzare un'altra applicazione, APPN per prima cosa ricerca la LU destinataria in tale lista.

Se la LU non viene trovata, la richiesta viene inviata al NN. Ogni NN conosce le LU degli EN e dei nodi LEN da esso serviti, oltre alle LU di alcune destinazioni pre-programmate (le più utilizzate) e alle LU precedentemente richieste (mantenute in una cache).

Se la LU viene trovata nella lista del NN, il NN verifica l'informazione, prima di utilizzarla, con una ricerca diretta (figura 18.15).

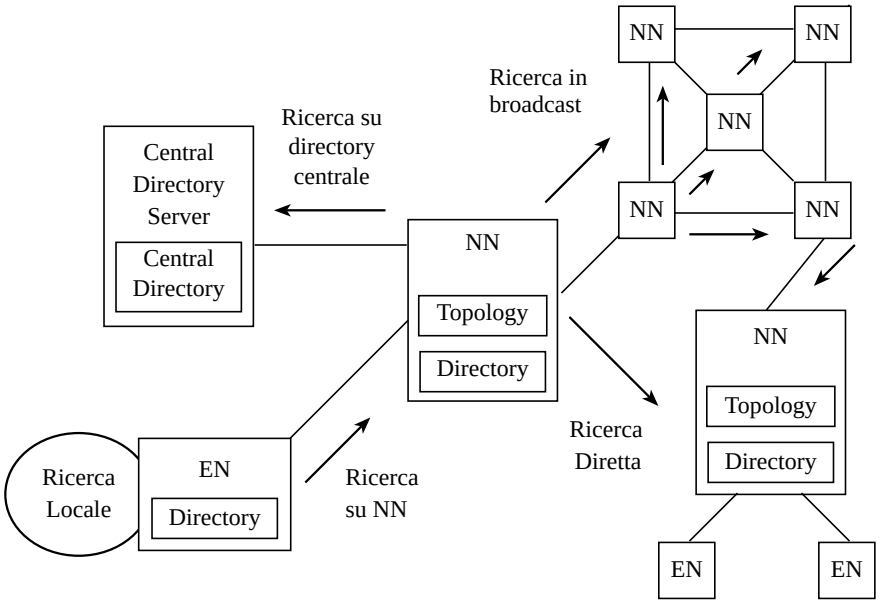


Fig. 18.15 - Ricerca su servizio di directory.

Se la LU non è nota al NN, questo inizia una ricerca in broadcast inviando la richiesta ad altri NN.

Opzionalmente può essere presente un directory centrale che contiene informazioni di importanza aziendale: anche su di esso viene effettata la ricerca. Il servizio di directory centrale è offerto dalle versioni del VTAM che supportano APPN.

Il servizio di directory aumenta notevolmente la flessibilità della rete: non occorre più preoccuparsi se le applicazioni vengono spostate su altri elaboratori, perché la rete tiene conto dinamicamente della loro localizzazione e i NN forniscono su richiesta tale informazione agli EN.

18.3.8 Route selection

Determinato quale nodo ospita la LU con cui si vuole stabilire una sessione, occorre determinare quale sia l'instradamento migliore per raggiungere quel nodo.

Gli applicativi specificano in fase di bind della sessione un *mode name* e l'indirizzo di destinazione. Il mode name indica la classe di servizio richiesta e la priorità di trasmissione. La classe di servizio include a sua volta parametri quali la sicurezza dell'instradamento richiesto, la banda, il ritardo di propagazione massimo,

il costo, ecc.

È inoltre possibile assegnare ai NN un valore di resistenza (*resistance*). I nodi con basso valore di resistenza sono preferiti nella scelta degli instradamenti. Esempi di nodi a cui assegnare bassi valori di resistenza sono i router, mentre esempi di nodi a cui assegnare un alto valore di resistenza sono gli host: in questo modo gli host entrano a far parte solo dei cammini di backup della rete e gli applicativi che vi risiedono non sono penalizzati dal traffico in transito.

Il servizio di route selection evita anche di attraversare nodi intasati e ripartisce il traffico in modo casuale su più cammini equivalenti.

Il servizio di route selection, basandosi sull'indirizzo di destinazione, sulla classe di servizio richiesta e sullo stato della rete, sceglie un dato instradamento che rimarrà immutato per tutta la durata della sessione. Tale instradamento viene notificato al nodo richiedente tramite un RSCV (*Route Selection Control Vector*) che è l'insieme dei nodi e dei link da attraversare.

Le sessioni hanno un identificatore univoco su tutta la rete detto FQPCID (*Fully Qualified Procedure Correlation IDentifier*) assegnato dal nodo che ha richiesto la sessione (figura 18.16).

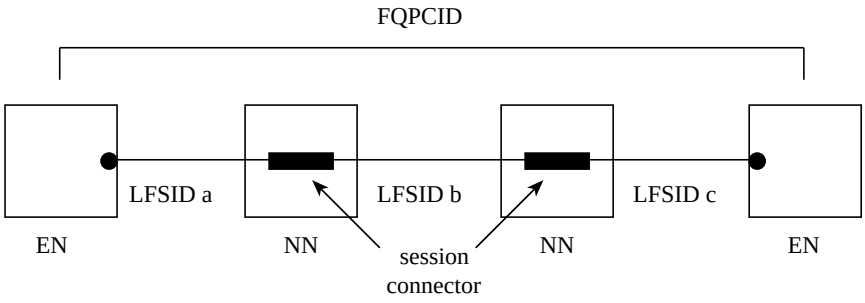


Fig. 18.16 - FQPCID e LFSID.

Il FQPCID è usato pricipalmente per scopi di gestione (*management*) e non per instradare i messaggi sulla rete. Questo secondo compito è affidato al LFSID, descritto nel seguente paragrafo.

18.3.9 ISR

I NN hanno anche un modulo di ISR (*Intermediate Session Routing*) che agisce come router per i pacchetti generati da applicazioni residenti su altri nodi.

L'ISR, oltre ad instradare i pacchetti, offre servizi di recupero degli errori, di controllo adattativo di flusso e delle congestioni (adaptative pacing), e di segmentazione e riassemblaggio. Quindi il modulo ISR raggruppa al suo interno problematiche tipiche del livello Network e anche del livello Transport.

ISR usa i pacchetti di tipo FID2 e fornisce un servizio di tipo connesso. Nei servizi di tipo connesso gli indirizzi del mittente e del destinatario vengono specificati solo al bind della sessione e quindi al servizio di route selection.

Il route selection restituisce una routing label che viene usata per identificare tutti i pacchetti appartenenti a quella sessione. Le routing label sono lunghe 17 bit e si chiamano LFSID (*Local Form Session IDentifier*).

Durante la fase di route selection su ogni NN attraversato dalla sessione viene creata una entry in una routing table (che è diversa dal database topologico) detta *session connector* (figura 18.17).

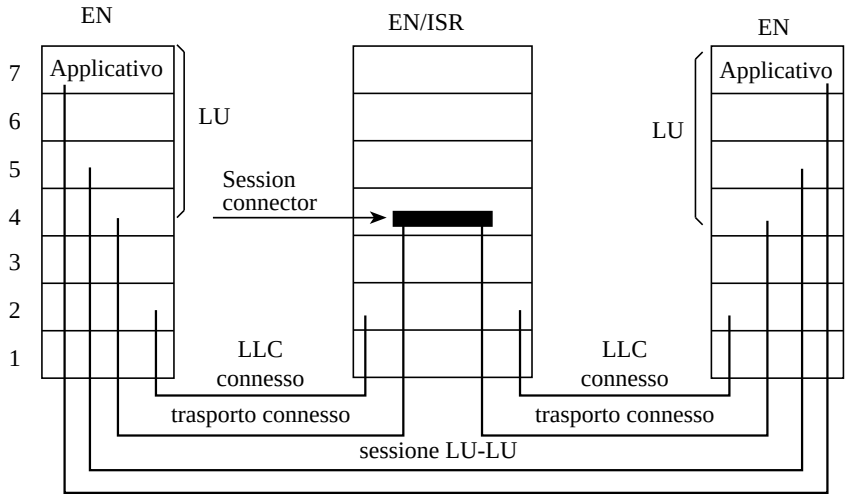


Fig. 18.17 - APPN ISR.

APPN/ISR usa una tecnica di instradamento di tipo label swapping: ogni NN APPN legge il LFSID del pacchetto ricevuto e, tramite il session connector, determina su quale linea ritrasmettere il pacchetto ricevuto e con quale nuovo LFSID identificarlo. In questo modo gli LFSID devono essere univoci solo all'interno di una linea (figura 18.18).

I link APPN sono detti TG (Transmission Group) come in SNA, ma non è ammesso avere più linee all'interno di un TG. Per questa ragione in APPN i termini

TG, link e linea sono sinonimi.

La figura 18.18 mostra il cammino tra EN1 e EN2. EN1 genera i pacchetti con LFSID=A e li invia sul TG1. Il NN 3 riceve i pacchetti, consulta la tabella di instradamento associata a TG1, ricerca il session connector con IN-LFSID=A, lo trova, genera un nuovo pacchetto con LFSID=OUT-LFSID, cioè B, e lo trasmette sul TG2.

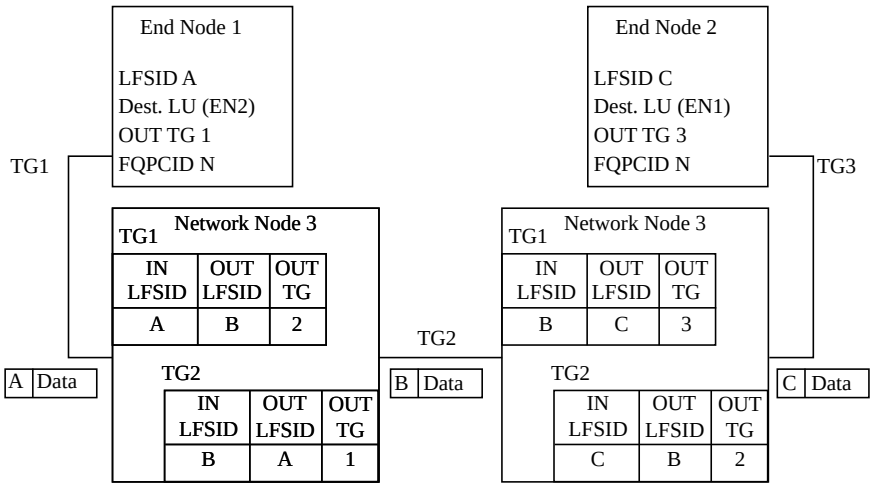


Fig. 18.18 - ISR label swapping.

Il procedimento si ripete su NN 4 che cambia lo LFSID in C e trasmette il pacchetto su TG3.

Si noti che per ogni sessione devono esistere due session connector: uno per l'instradamento in una direzione, l'altro per l'instradamento nella direzione opposta. Ad esempio, quando EN 2 invia una risposta, questa arriva a NN 4 tramite TG3, e quindi la tabella di instradamento che si consulta è quella associata a TG3.

Gli LFSID sono scelti dai nodi APPN dinamicamente, anche se nodi pre-APPN possono avere LFSID preassegnati.

APPN/ISR è in grado di convivere con altri protocolli di Network (es: IP e OSI) sugli stessi link, usando i servizi offerti da 802.2 (LLC) sulle reti locali, da PPP sui link HDLC e da Frame Relay.

Inoltre, poiché APPN utilizza lo stesso protocollo FID2 di subarea SNA, il traffico APPN può convivere con il traffico pre-APPN (ad esempio, di tipo 3270) sulle stesse linee.

18.3.10 Indirizzi APPN

Gli indirizzi APPN sono associati alle NAU (*Network Accessible Unit*). Essi sono stringhe di caratteri alfanumerici che costituiscono uno spazio di indirizzamento di miliardi di nodi e reti. Gli indirizzi APPN sono organizzati in network che possono avere sino a 10000 nodi (limite tipico degli algoritmi link state packet). Lo schema è simile a quello delle aree OSI e lo spostamento di un nodo all'interno di una network non implica nessuna modifica a livello di definizioni di sistema.

L'indirizzo di una NAU è quindi composto da due parti NETID.NAUNAME:

- NETID: identifica la network con una stringa da 1 a 8 caratteri alfanumerici;
- NAUNAME: identifica la NAU all'interno della network con una stringa da 1 a 8 caratteri alfanumerici.

Un nodo APPN può avere molte LU, ma un solo CP. In questo caso ogni LU e il CP hanno un indirizzo diverso. Tuttavia, ad eccezione dei mainframe, molti nodi APPN hanno una sola LU e l'indirizzo del CP è anche usato come indirizzo della LU.

Questo è reso possibile dal fatto che APPC su APPN ammette di avere più sessioni con una singola LU, possibiltà che non esisteva nelle reti subarea SNA.

18.3.11 Dependent LU

APPN è stata concepita principalmente per trasportare traffico di tipo APPC e quindi associato alle LU 6.2, anche dette independent LU. Tale traffico è generato da stazioni "intelligenti" quali i personal computer, e sarà in futuro indubbiamente il tipo di traffico dominante.

Tuttavia molte applicazioni sviluppate per reti subarea SNA utilizzano le DLU (*Dependent Logical Unit*), cioè le LU di tipo 0, 1, 2 e 3. Il traffico più rilevante di questo tipo è generato dai terminali "stupidi" 3270.

Le DLU, per poter funzionare correttamente, dipendono dallo SSCP e necessitano delle sessioni SSCP-PU e SSCP-LU. Queste si possono stabilire solo se esiste una connessione diretta tra il nodo di tipo 1 o 2 (cluster controller) e il nodo di subarea di tipo 4 (FEP) o 5 (host); l'interposizione di altri NN APPN non è ammessa.

Per trasportare il traffico delle DLU su una rete APPN, IBM offre due possibilità:

- convertire il traffico a independent LU;
- utilizzare un Dependent LU Requester/Server.

La prima possibilità implica la modifica del software applicativo e quindi è tipicamente rifiutata dagli utenti con un'unica grande eccezione: il traffico 3270.

18.3.12 APPC3270

APPC3270 è un programma applicativo per personal computer che trasporta il traffico 3270 su una LU 6.2 e quindi su una rete APPN. Simile all'applicativo TN3270 che trasporta il traffico 3270 su TCP/IP, anche APPC3270 richiede che le stazioni di lavoro siano dei personal computer e non dei terminali 3270 veri e propri.

18.3.13 Dependent LU Requester/Server

Il DLUR (*Dependent LU Requester/Server*) è la soluzione più generale e flessibile al problema del trasporto del traffico generato dalle DLU su una rete APPN. Si tratta di un software composto da due moduli:

- il DLUS (*DLU Server*) che risiede sul VTAM di un host;
- il DLUR (*DLU Requester*) che risiede su un cluster 3174, su uno SNA gateway o su altri dispositivi periferici.

Tra i DLUR e i DLUS vengono realizzate delle sessioni APPC che creano l'adiacenza logica richiesta dal traffico di controllo SSCP, indipendentemente dalla topologia della rete APPN.

La figura 18.19 mostra un esempio di uno SNA gateway che ha un DLU requester che è in sessione con il DLU server realizzato dal VTAM sull'host. Tale VTAM scambia i dati di cross-domain tramite la rete APPN utilizzando il modulo SSE (*System Service Extension*).

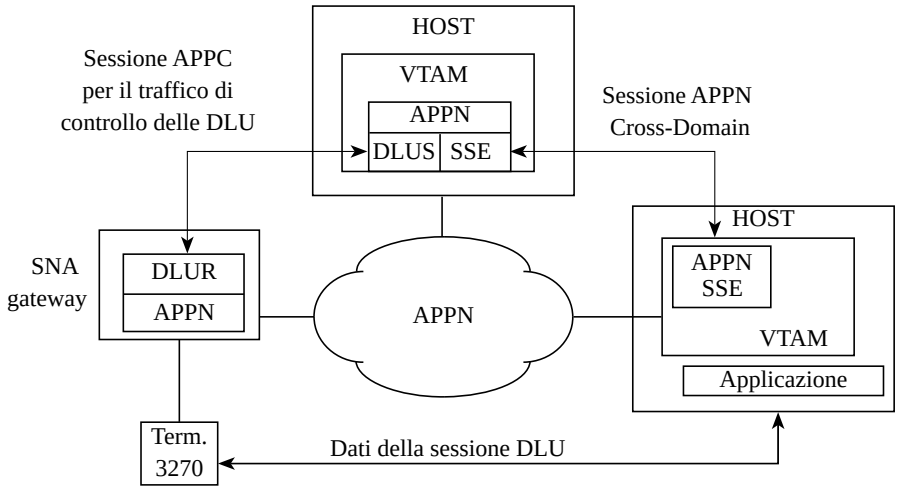


Fig. 18.19 - DLU Requester/Server.

Il vantaggio di questo approccio consiste nella totale trasparenza agli applicativi e nella totale indipendenza dai dispositivi hardware.

18.4 LA RETE APPN+/HPR

HPR (*High Performance Routing*), noto anche con la sigla di APPN+, è una evoluzione di APPN che migliora i livelli network e transport, pur mantenendo la totale integrazione con ISR.

HPR introduce il concetto di *dynamic rerouting*, permettendo il reinstradamento dinamico di una sessione, senza che i livelli superiori se ne accorgano. L'assenza di questa prestazione era una grave carenza in APPN, in quanto tutte le altre principali architetture di rete (es: TCP/IP e OSI) ne sono dotate.

HPR è in grado di usare a livello 2 sia la modalità connessa, sia la modalità non connessa, in funzione dell'affidabilità del link. Più l'affidabilità è alta, meno appropriato diventa l'utilizzo di un protocollo connesso.

HPR mantiene i concetti di stabilità del routing, di supporto della priorità di trasmissione e di classe di servizio, tipici di SNA e APPN.

HPR può coesistere lungo un cammino con ISR come evidenziato in figura 18.20. I vantaggi di HPR iniziano ad evidenziarsi quando ci sono più di due link consecutivi e quindi almeno tre nodi consecutivi in grado di utilizzarlo.

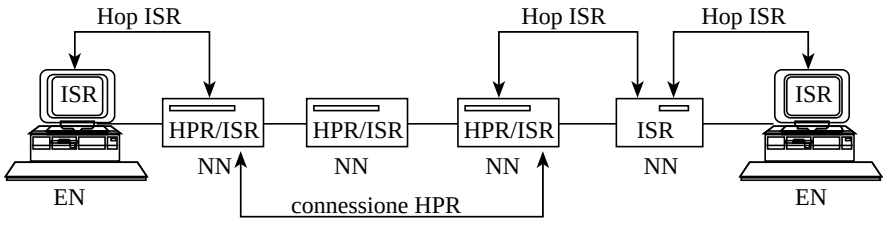


Fig. 18.20 - Integrazione di ISR e HPR.

HPR è preferito per collegamenti a basso tasso di errore (migliore di 10^{-7}) e ad alta velocità, quali le LAN e i collegamenti digitali ad alte prestazioni (es: CDN E1 a 2Mb/s). Su collegamenti analogici a bassa velocità ed alto tasso di errore ISR continua ad essere preferibile.

HPR non usa il LFSID e il label swapping. Invece adotta una tecnica di source

routing derivata da quella dei source routing bridge di IEEE 802.5. Il pacchetto, quando viene generato, contiene nell'header del pacchetto di network la lista dei TG da attraversare (figura 18.21).

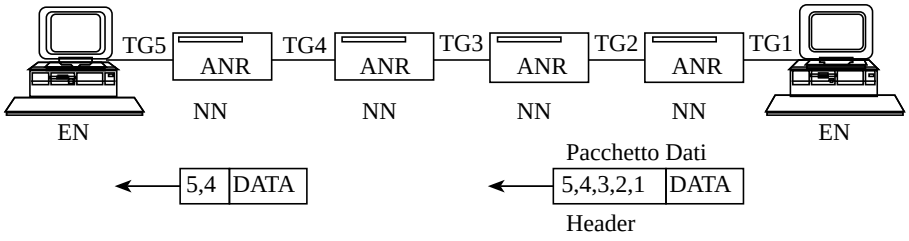


Fig. 18.21 - Esempio di routing HPR.

Ogni router elimina dalla lista il TG da cui ha ricevuto il pacchetto e lo instrada verso il nodo successivo.

HPR introduce un nuovo tipo di pacchetto detto PTM (*Packet Transfer Mode*) e un nuovo formato per l'header detto FID5 (*Format IDentifier 5*).

L'header FID5 è leggemente più grande dell'header FID2 usato da APPN, ma il tempo di elaborazione ad ogni nodo intermedio è ridotto rispetto a quello di ISR.

Il FID5 rimpiazza anche il FQPCID con un nuovo *session address.*

HPR può operare anche sui MLTG (*Multi Link Transmission Group*), cioè un insieme di link paralleli trattato come un unico link (concetto simile al TG di SNA, che però in APPN è limitato ad un singolo link).

HPR introduce anche i concetti di ANR (*Automatic Network Routing*), RTP (*Rapid Transport Protocol*) e ARB (*Adaptative Rate Base congestion control*).

18.4.1 Automatic Network Routing

ANR è un protocollo di network source routing semplice, non connesso, senza stati (*stateless*) e ad alta efficienza. ANR scarta i pacchetti entranti in presenza di congestioni e ordina i pacchetti da trasmettere in funzione della loro priorità.

ANR utilizza non LFSID, ma le informazioni di source routing contenute nell'header del pacchetto e derivate dallo RSCV.

ANR esiste e svolge le sue funzioni su ogni nodo di un cammino HPR, a differenza di RTP che opera solo sui nodi terminali del cammino.

18.4.2 Rapid Transport Protocol

RTP è un protocollo di trasporto connesso che opera solo sui nodi finali di una connessione HPR e non su quelli intermedi. Da questo punto di vista si può evidenziare una similarità tra IP e ANR e tra TCP e RTP.

RTP è un'evoluzione del protocollo XTP (*eXpress Transfer Protocol*) sviluppato dalla Protocol Engines Inc., e proposto, ma non accettato, come LLC type 4.

RTP è stato progettato per link più veloci, a basso tasso di errore, per calcolatori con maggiore memoria e schede di rete ad alto throughput. Il numero di acknowledgement, di stati del protocollo, di controlli di flusso e, in generale, di handshake del protocollo sono ridotti.

RTP determina la massima dimensione dei pacchetti sull'intero cammino e segmenta i pacchetti che eccedono tale massimo prima del primo hop. Nessuna elaborazione viene fatta da RTP sui nodi intermedi. Il RTP destinatario riassembla i pacchetti.

RTP effettua il controllo e il recupero degli errori di trasmissione. Il recupero avviene tramite uno schema di *selective retransmission* in cui solo il pacchetto errato viene ritrasmesso, mentre la modalità classica è il "go back N" cioè riprendere a ritrasmettere dal pacchetto errato, ignorando pacchetti successivi già arrivati a destinazione correttamente.

RTP realizza anche una tecnica di reinstradamento dinamico della connessione in caso di problemi lungo il cammino. Dopo un certo numero di tentativi di trasmissione senza successo, RTP chiede al control point di APPN di calcolare un nuovo RSCV. La sessione non si avvede del cambiamento di instradamento.

18.4.3 Adaptative Rate Base

Per gestire link ad alta velocità in modo efficiente è necessario disporre di algoritmi di controllo delle congestioni e del flusso di tipo end-to-end. HPR comprende un algoritmo detto ARB (*Adaptative Rate Based*) *congestion control* che modifica dinamicamente la quantità di dati inviati dal mittente nell'unità di tempo in funzione delle informazioni di stato ricevute. Queste riguardano sia lo stato della rete (*congestion control*) sia lo stato del nodo ricevente (*flow control*).

ARB è stato dimostrato essere più efficiente degli algoritmi attualmente usati, quali lo *slow-start* adottato da TCP.

18.5 LA RETE BBNS

Il BBNS *(Broad Band Network Service)* è stato annuciato da IBM nel luglio 1993 ed è caratterizzato dall'integrazione con ATM (si veda capitolo 19). BBNS definisce un nuovo control point (tabella 18.2) ed ammette come nuovo formato di pacchetto la cella ATM (53 byte).

Le funzioni di instradamento sono quelle standard di ATM, più quelle offerte da PTM.

BBNS aggiunge ai servizi ATM altri servizi presenti nelle reti IBM, quali la qualità del servizio, l'allocazione di banda, i servizi di directory multiprotocollo e la gestione dei gruppi di multicast.

BBNS, basandosi su ATM, non solo fornisce trasferimento dati per protocolli IBM e non, ma può trasportare anche altri tipi di informazioni multimediali, quali il video e la voce.

BIBLIOGRAFIA

[1] Apertus Technologies Inc., "APPN Primer: A Guide to Advanced Peer-to-Peer Networking", New York, USA, 1994.

[2] Marcia L. Peters, "APPN and Extensions: The New Industry Standard for SNA Internetworking", IBM Corp., Research Triangle Park, NC, USA.

[3] James P. Graym, Marcia L. Peters, "A Preview of APPN High Performance Routing", IBM Corp., Research Triangle Park, NC, USA, July 1993.

[4] R. Dixon, D. Kushi, "RFC 1434: Data Link Switching: Switch-to-Switch Protocol", March 1993.

[5] R.M. Sanders, A.C. Weaver, "The Xpress Transfer Protocol (XTP) - A tutorial, Computer Network Laboratory, Dept. of Computer Science, University of Virginia, TR-89-10, January 1990.

[6] R.F Chang, J. P. Gray, L. Huynh, "Comparison of Congestion Control Performance of APPN+ and TCP", IBM Corp., Unclassified, Technical Report 29.1490, December 1992.

19

B-ISDN E ATM

19.1 INTRODUZIONE

Attualmente esistono diverse reti di telecomunicazioni, ciascuna specializzata nel fornire un dato servizio: ad esempio la telefonia, il telex, la televisione via cavo, i dati a commutazione di circuito e a commutazione di pacchetto.

Un primo passo verso l'integrazione delle reti è stato compiuto con l'ISDN (*Integrated Services Digital Network*), il quale è in grado di veicolare fonia, dati e video a bassa velocità utilizzando una rete numerica con una banda da 64 Kb/s a 2 Mb/s, assegnabile al servizio richiedente in multipli interi di 64 Kb/s (si veda il paragrafo 12.7).

Le esigenze di mercato spingono verso l'introduzione di una serie di servizi a più larga banda mirati ad utenze sia di tipo affari, ad esempio, trasmissione dati ad elevata velocità, full-motion e full-color video, videoconferenza, interconnessione di LAN e workstation, sia di tipo domestico, ad esempio Video On Demand, Hi-Fi audio e games downloading.

Per rispondere a detta esigenza gli organismi di standardizzazione internazionale hanno discusso come far evolvere ISDN verso una rete a larga banda (*Broadband ISDN* o *B-ISDN*) capace di gestire in modo flessibile il maggior numero possibile di servizi di telecomunicazione [1]. Questi servizi, facendo riferimento alla figura 19.1, possono essere classificati come segue:

- *bassissima velocità*: telemetria, telecontrollo, teleallarmi;
- *bassa velocità*: fonia, fax, POS (Point Of Sale), sessioni di lavoro con host remoti, transazioni remote come prenotazioni su linee aeree, ecc.;
- *media velocità*: Hi-Fi audio, video a bassa velocità, fax ad alta risoluzione (HQ fax);
- *alta velocità*: interconnessione di LAN, file transfer;

- *Altissima velocità*: broadcast video, video on demand, televisione ad alta definizione (HDTV), video library, videoconferenza.

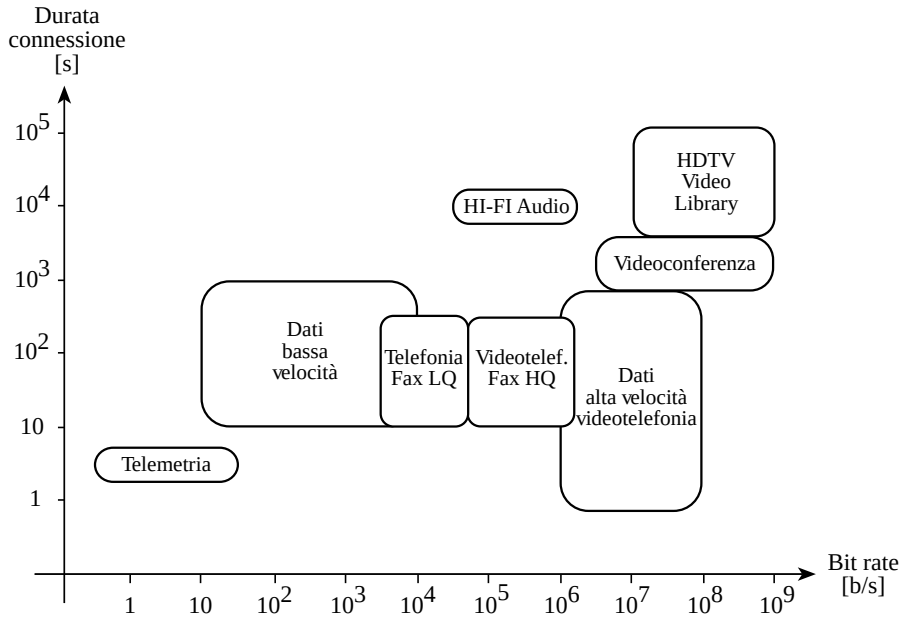


Fig. 19.1 - Caratteristiche delle sorgenti di traffico.

Data la grande varietà dei servizi da fornire, sia in termini di velocità, sia di durata della comunicazione, il B-ISDN deve essere il più possibile:

- *flessibile, scalabile e indipendente dall'applicazione:* in modo da poter essere aggiornato in futuro con l'introduzione di nuovi servizi, preservando nel tempo gli investimenti;
- *efficiente:* dovendo far condividere le risorse di rete ad una pluralità di servizi senza che le prestazioni di questi vengano a risentirne;
- *economico:* i costi di progettazione, installazione, gestione e manutenzione di B-ISDN devono essere inferiori al costi aggregati delle reti che sostituisce.

Lo schema generale di una interconnessione B-ISDN è mostrato in figura 19.2, dove è possibile osservare che il bus S tipico dell'ISDN tradizionale (*Narrow Band ISDN*) continua ad esistere e prende il nome di S_0 ed è affiancato dai due bus S_B e S_D tipici del B-ISDN. Il bus S_B ha uno scopo simile a quello del bus S_0, cioè fornire servizi interattivi, ma a larga banda. Il bus S_D serve invece per i servizi

distributivi in cui un segnale a larga banda viene distribuito ad un ampio numero di terminali (ad esempio, televisione via cavo).

Dalla figura 19.2 emerge inoltre come per realizzare B-ISDN le velocità trasmissive debbano essere comprese nell'intervallo 150 Mb/s - 600 Mb/s.

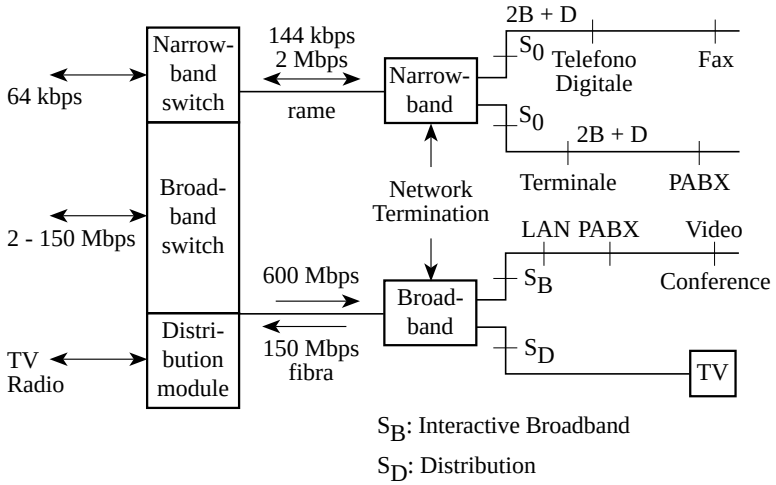


Fig. 19.2 - Connessione B-ISDN.

Nel 1987 il CCITT ha deciso di basare il B-ISDN, per quanto riguarda gli aspetti trasmissivi su SDH (si veda il paragrafo 12.6) e per quanto riguarda gli aspetti di commutazione su *ATM (Asynchronous Transfer Mode).*

Questa decisione ha fatto di ATM lo standard universalmente accettato per le reti nel mercato delle telecomunicazioni, dei calcolatori elettronici e dell'elettronica di consumo. Il grande mercato potenziale di ATM ha spinto un numero elevato di costruttori ad impegnarsi in modo significativo sia nella realizzazione di apparati e componenti ATM, sia nella veloce definizione degli standard, tramite una associazione di costruttori e utenti, creata nel novembre 1991, denominata *ATM Forum* .

ATM Forum raggruppava a giugno '94 570 membri, tra cui 168 costruttori, 69 utenti e 333 ascoltatori. ATM Forum ha lo scopo di accelerare il processo di standardizzazione di ATM, con particolare riferimento all'interoperabilità dei prodotti, come specificato nell'atto costitutivo: "An Industry Group of Vendors, Service Providers and Network Users that Formulate Implementations of the ATM Standards".

Oltre al ruolo rivestito nell'ambito di B-ISDN, è certo che ATM sarà utilizzata come

infrastruttura di trasporto per reti di tipo privato e come struttura di interconnessione intra-dispositivo. Ad esempio già oggi si costruiscono commutatori Frame Relay e concentratori di rete locale (HUB) aventi una struttura interna realizzata con tecnica ATM. Molti costruttori di calcolatori hanno annunciato che nel prossimo futuro abbandoneranno le reti locali tradizionali a favore di quelle ATM.

19.2 FONDAMENTI DELLA TECNICA ATM

La tecnica ATM si occupa del trasporto di informazioni in forma numerica, sia di tipo continuo, come fonia e video, sia di tipo discontinuo (a burst), come il traffico dati generato dalle LAN. Questo trasporto viene effettuato su una rete costituita da un insieme di nodi di commutazione e da un insieme di nodi terminali (figura 19.3).

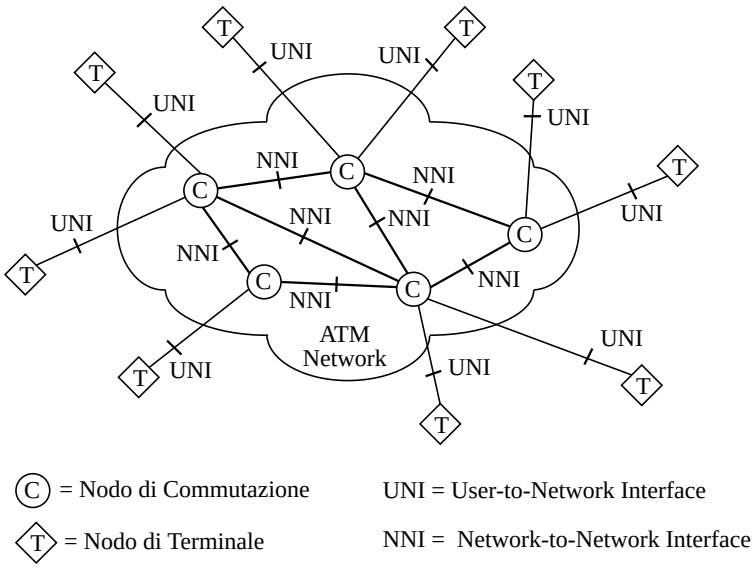


Fig. 19.3 - Struttura di una rete ATM.

I nodi di commutazione, detti brevemente commutatori, sono collegati tra loro con linee punto-punto secondo una topologia assolutamente arbitraria, che ammette la presenza di magliature. I nodi terminali invece possono essere collegati unicamente ai nodi di commutazione, anch'essi con linee punto-punto, con una topologia stellare.

L'interfaccia tra commutatore e terminale utente viene chiamata *User-to-Network*

Interface (UNI) [4] mentre quella tra commutatore e commutatore prende il nome di *Network-to-Network Interface* (NNI). Le UNI e la NNI sono i principali standard su cui basarsi per realizzare una rete ATM ed esistono standard per queste interfacce in ambito pubblico e privato, come mostrato dalla figura 19.4.

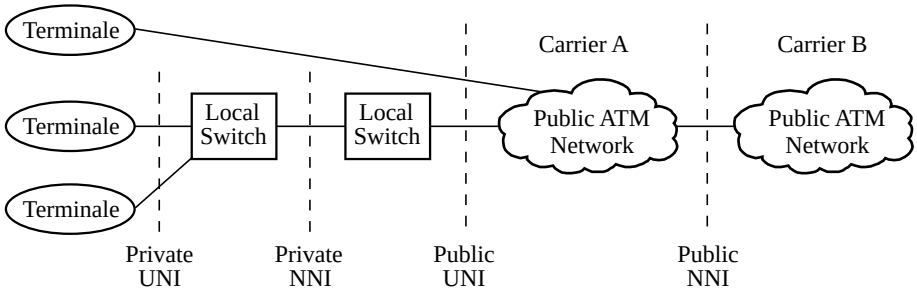


Fig. 19.4 - Interfacce pubbliche e private.

Ovviamente un alto livello di standardizzazione di queste interfacce è auspicabile in quanto alla base dell'interoperabilità tra apparati di costruttori diversi.

La comunicazione tra due terminali utente avviene su una *connessione virtuale*, cioè su un canale logico. L'informazione viene instradata su un percorso fisico associato alla connessione virtuale sotto forma di una sequenza di unità informative elementari dette *celle*.

Le celle ATM possono essere di due tipi (si veda la figura 19.5), a seconda dell'interfaccia su cui transitano. Entrambi i tipi di celle hanno una lunghezza fissa pari a 53 byte, di cui 5 dedicati all'intestazione (Header) e 48 al campo informazioni (Payload).

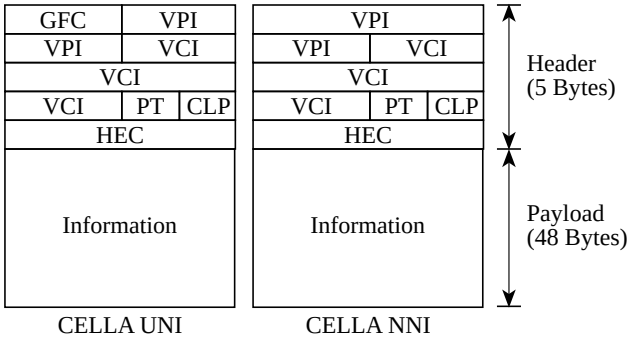


Fig. 19.5 - Formati delle celle ATM.

Il significato dei campi dell'intestazione è il seguente:

- GFC (*General Flow Control*): è lungo 4 bit nelle celle UNI ed è assente in quelle NNI. Dovrebbe essere utilizzato per il controllo del traffico e delle congestioni, ma attualmente non ne sono ancora state definite le funzioni. Questo campo è presente solo nelle celle UNI perché la gestione del traffico è solo di competenza di questa interfaccia;
- VPI (*Virtual Path Identifier*): è lungo 8 bit nelle celle UNI e 12 bit in quelle NNI. Costituisce una parte dell'identificatore di connessione virtuale. Identifica un gruppo di canali virtuali (è l'analogo del *fascio di circuiti* nella commutazione di circuito);
- VCI (*Virtual Channel Identifier*): la sua lunghezza è pari a 16 bit per entrambi i tipi di celle. Costituisce la restante parte dell'identificatore di connessione virtuale. Identifica un canale virtuale tra due stazioni nell'ambito di un percorso virtuale;
- PT (*Payload Type*): è lungo 3 bit per entrambe le celle. Indica se il campo dati trasporta effettivamente dati utente oppure informazioni di servizio per la gestione della rete;
- CLP (*Congestion Loss Priority*): un solo bit di lunghezza. Indica se una cella può essere scartata da un commutatore qualora si verifichino condizioni di congestione;
- HEC (*Header Error Control*): lunghezza 8 bit. È il CRC calcolato sulla sola intestazione della cella e permette la correzione di un errore singolo e la rilevazione di un errore doppio nell'header della cella.

I commutatori hanno il compito di trasferire le celle provenienti da un canale in ingresso verso un canale in uscita. Questa operazione viene svolta in un modo semplice e veloce. Infatti, l'intestazione di ogni cella contiene un *identificatore di connessione virtuale*, detto anche *etichetta*, che è costituito dall'insieme di VPI/VCI e serve a determinare la connessione a cui una cella appartiene. L'etichetta, essendo costituita da un numero limitato di bit, identifica in modo univoco una connessione solo all'interno di un canale, quindi nel passaggio da un canale di ingresso ad un canale di uscita deve essere opportunamente sostituita. Per ogni linea di ingresso di un nodo di commutazione, l'etichetta funge da puntatore ad una tabella di transcodifica (look-up) che contiene la nuova etichetta da porre nell'intestazione e la linea su cui la cella deve essere ritrasmessa. Una successione di cambi di etichetta (label swapping, si veda anche il paragrafo 14.1.1) e di linea determina di conseguenza il percorso di una cella all'interno della rete, dal terminale di origine a quello di destinazione. Se la connessione è di tipo multicast allora l'etichetta individua un

insieme di nuove etichette e di linee di uscita e la cella sarà replicata un numero di volte pari alle possibili destinazioni.

Un commutatore ATM (figura 19.6) deve quindi essere in grado di effettuare, per ogni cella che riceve, due operazioni:

- *Commutazione di multiplex*: trasferire fisicamente una cella da una terminazione di ingresso ad una o più terminazioni di uscita;
- *Commutazione di etichetta:* variare l'identificatore di connessione virtuale da quello valido sul multiplex di ingresso a quello valido sul multiplex di uscita.

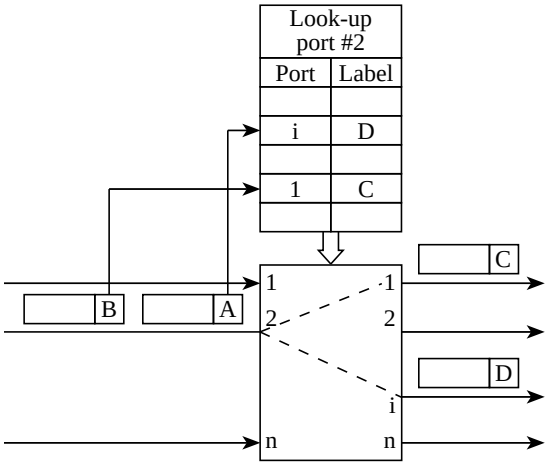


Fig. 19.6 - Nodo di commutazione ATM.

Queste due funzioni, essendo semplici ed operando su dati di dimensioni contenute e fisse, possono essere implementate interamente in hardware, rendendo così la commutazione estremamente veloce.

Le celle vengono trasmesse sulle linee con velocità trasmissive molto elevate (tipicamente maggiori o uguali a 155 Mb/s) e su una stessa linea possono transitare più connessioni virtuali. Più flussi di celle ATM possono essere riuniti in un unico flusso a velocità superiore attraverso un'operazione di *multiplazione* (figura 19.7).

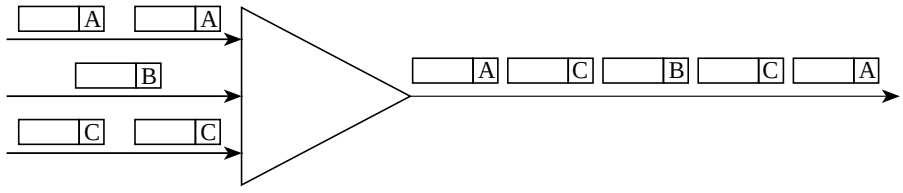


Fig. 19.7 - Multiplazione.

Tale multiplazione è *asincrona* in quanto non esiste alcuna relazione tra la posizione che occupa una cella nel flusso multiplato ed il flusso da cui la cella proviene. Di conseguenza la demultiplazione in ricezione avviene separando le celle in base al loro identificatore di connessione virtuale e non in base a informazioni temporali.

Esistono due tipi di connessioni virtuali: *Permanent Virtual Connections* (PVC) e *Switched Virtual Connections* (SVC). Le connessioni PVC vengono create dal gestore della rete con opportune operazioni di configurazione e sono l'equivalente di una linea dedicata tra due utenti. Le connessioni SVC sono invece create dinamicamente, su richiesta di un utente, mediante procedure di segnalazione, esattamente come nel caso di connessioni telefoniche commutate.

Ad una connessione virtuale è associato un percorso fisico sulla rete e la sua attivazione comporta la generazione di una nuova etichetta per ogni interfaccia che compone il percorso fisico e la configurazione delle tabelle di look-up nei commutatori attraversati.

Ad ogni connessione virtuale è inoltre associata una qualità del servizio*(QoS: Quality of Service)* che viene negoziata all'atto dell'instaurazione della connessione stessa. La qualità del servizio definisce dei parametri contrattuali tra il terminale e la rete ATM come, ad esempio, la banda desiderata, la priorità dell'informazione, il ritardo massimo ed il tasso di perdita delle celle. La qualità del servizio serve a caratterizzare il traffico affinché la rete possa trattarlo adeguatamente riservando ad esso opportune risorse.

Ad esempio, un traffico generato da una videoconferenza ha una banda ed una priorità molto elevate, non tollera ritardi che superino poche centinaia di millisecondi, ma sopporta dei tassi di perdita diversi da zero; per contro, un traffico causato dal back-up remoto di un file server ha esigenze di banda e di priorità abbastanza contenute, sopporta ritardi dell'ordine dei secondi, ma non tollera assolutamente la perdita di celle.

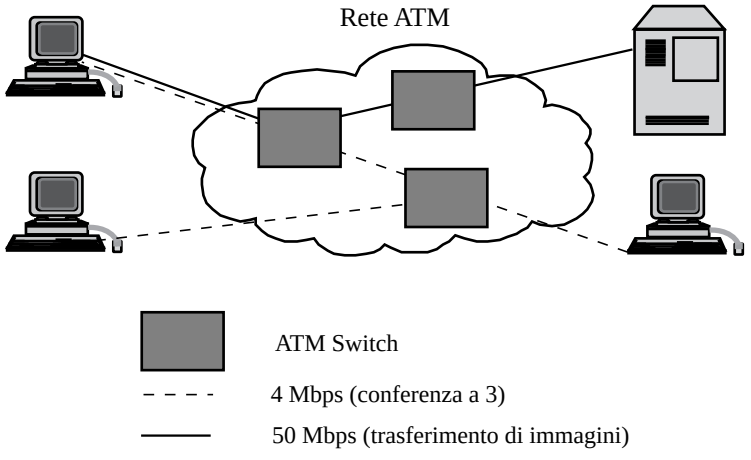


Fig. 19.8 - Connessioni virtuali.

La figura 19.8 mostra un esempio di due connessioni virtuali con QoS diverse. Una delle due connessioni è punto-punto, mentre l'altra è di tipo punto-multipunto.

19.3 ASPETTI DI INDIRIZZAMENTO

Per poter stabilire una connessione virtuale con un'altra stazione occorre che ogni stazione abbia un indirizzo ATM. Questo non deve essere confuso con il VPI/VCI: l'indirizzo ATM è un identificatore univoco a livello mondiale di una stazione ATM ed è utilizzato in fase di segnalazione per stabilire una SVC. Una volta creata la SVC, essa viene identificata dal VCI/VPI assegnato dalla rete durante la segnalazione.

Un indirizzo ATM deve:

- avere una struttura gerarchica che consenta di definire domini di routing e reti all'interno di questi;
- contenere un identificatore unico ed invariante della stazione, incorporato nell'hardware ed assegnato da una autorità internazionale che ne assicuri l'unicità (esattamente come accade per l'indirizzo di livello MAC delle LAN Ethernet);
- essere creato dinamicamente quando una stazione viene connessa ad una data porta di un dato commutatore.

Per soddisfare questi requisiti gli indirizzi ATM hanno una lunghezza fissa pari a 20 ottetti e sono basati sugli indirizzi NSAP di OSI [6] (si veda il paragrafo 17.8). Sono ammessi tre formati come evidenziato in figura 19.9.

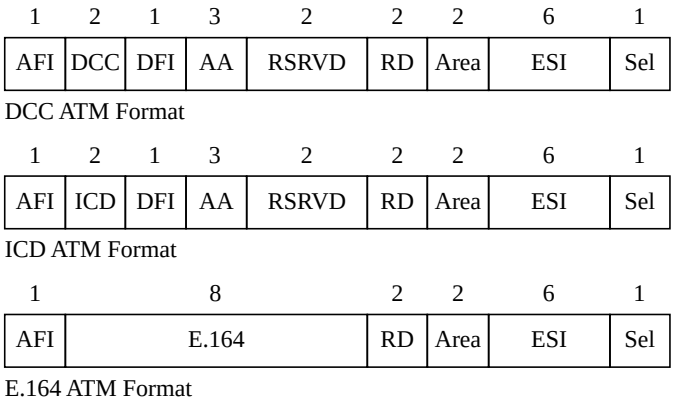

1 2 1 3 2 2 2 6 1
AFI DCC DFI AA RSRVD RD Area ESI Sel
DCC ATM Format
1 2 1 3 2 2 2 6 1
AFI ICD DFI AA RSRVD RD Area ESI Sel
ICD ATM Format
1 8 2 2 6 1
AFI E.164 RD Area ESI Sel
E.164 ATM Format

Fig. 19.9 - Indirizzi ATM.

Gli indirizzi E.164 sono principalmente usati per le reti ATM pubbliche, mentre gli ICD e i DCC sono utilizzate per le reti private.

Il significato dei campi è spiegato in modo integrativo a quanto già detto nel paragrafo 17.8:

- AFI (*Authority and Format Identifier*): assume il valore 39 nel caso DCC ATM format, 47 nell'ICD ATM format e 45 nell'E.164 ATM format.
- DCC (*Data Country Code*): codice della nazione che ha assegnato l'indirizzo in accordo allo standard ISO 3166 (per le codifiche dei principali paesi si veda la tabella 17.2).
- ICD (*International Code Designator*): identificatore di una organizzazione unico a livello mondiale.
- E.164: numero telefonico per ISDN.
- DFI (*Domain specific part Format Identifier*): specifica la struttura, il significato semantico e i requisiti amministrativi dei restanti campi a destra del DFI.
- AA (*Administrative Authority*): identifica quale autorità amministrativa è responsabile dell'assegnazione dei restanti campi a destra del campo AA.
- RSRVD (*Reserved*): riservato per usi futuri.
- RD (*Routing Domain*): identifica il dominio di routing all'interno di una organizzazione.
- *Area*: identifica una rete all'interno di un dominio di routing.
- ESI (*End System Identifier*): identifica una stazione ATM all'interno di una rete; normalmente è scritto in una ROM della scheda ATM.
- Sel (*Selector*): non utilizzato per il routing ATM, a disposizione della stazione ATM.

Dato che una stazione può essere posizionata o spostata in un qualunque punto della rete in un qualunque momento, è indispensabile la presenza di un protocollo di configurazione automatica che consenta:

- alla stazione di rilevare la sua posizione apprendendo la parte iniziale dell'indirizzo (da AFI ad Area) e completandolo con l'ESI;
- alla rete di rilevare l'indirizzo ATM della stazione per aggiornare i database di instradamento.

I database di instradamento rivestono un ruolo fondamentale nell'instaurazione delle connessioni virtuali e possono essere gestiti in vari modi: la proposta a livello di P-NNI è di utilizzare un algoritmo di tipo link state packet (si veda il paragrafo 14.7) e un protocollo tipo OSPF o IS-IS* per costruire ed aggiornare dinamicamente tali database.

* OSPF (*Open Shortest Path First*) e IS-IS (*Intermediate System to Intermediate System*) sono due dei protocolli di routing maggiormente utilizzati sulle reti TCP/IP ed OSI.

19.4 ASPETTI ARCHITETTURALI

Si è precedentemente accennato al fatto che un nodo di commutazione ATM deve svolgere due funzioni: un cambiamento di multiplex, che corrisponde nella normale commutazione di circuito ad una commutazione spaziale ed un cambiamento di etichetta, che è l'analogo di una commutazione di slot nella tecnica TDM (*Time Division Multiplexing*). In ATM infatti, l'appartenenza di una cella ad una data connessione è riconoscibile non dalla sua posizione temporale sul flusso in ingresso (l'arrivo di una cella è un evento asincrono), ma dai valori di VPI/VCI (cioè dall'etichetta).

La funzione di traslazione di etichetta viene realizzata fisicamente mediante una tabella di transcodifica (*look-up table*) associata a ciascuna porta di ingresso del commutatore. A tale tabella si accede con la vecchia etichetta per estrarre quella nuova, mentre la commutazione di multiplex viene implementata per mezzo di una struttura di commutazione spaziale dotata di *buffer*, cioè di memorie in cui le celle vengono immagazzinate in attesa della commutazione per periodi di tempo dalla durata non deterministica, dipendenti dalle condizioni di carico della rete. Tali buffer sono indispensabili a causa delle caratteristiche intrinseche della tecnica asincrona: essi servono a risolvere i conflitti che si generano tra le celle che giungono su differenti porte di ingresso di un commutatore e sono destinate alla stessa porta di uscita.

In base al posizionamento dei buffer rispetto allo stadio spaziale si possono classificare le strutture di commutazione nel modo esposto nei seguenti sottoparagrafi.

19.4.1 Commutatori con buffer in ingresso

Ad ogni ingresso del commutatore è associato un buffer nel quale vengono memorizzate le celle che sono in attesa di essere instradate. A questa categoria appartengono i commutatori *Batcher-Banyan* (figura 19.10) così chiamati perché sono costituiti da una cascata di un ordinatore Batcher e da una rete Banyan* che è in grado di commutare senza blocco l'insieme di celle fornitegli dall'ordinatore Batcher.

* Un ordinatore Batcher è un dispositivo che presenta, su un insieme contiguo di uscite, le celle che si presentano ai suoi ingressi, ordinandole per indirizzo di destinazione crescente. Le reti Banyan costituiscono una famiglia di strutture di commutazione spaziale; sono realizzate interconnettendo secondo una certa topologia elementi di commutazione 2 x 2.

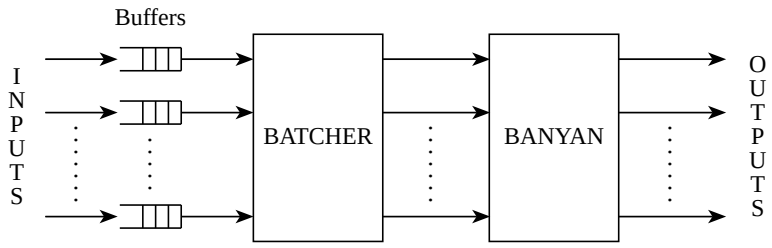


Fig. 19.10 - Commutatore Batcher-Banyan.

La struttura risultante è in grado, ad ogni ciclo di rete, di instradare in modo non bloccante un insieme di celle, a patto che queste siano dirette verso uscite differenti. Se ci sono dei conflitti, questi vengono risolti dai buffer, i quali memorizzano le celle contendenti e le fanno procedere nella struttura spaziale in base a determinati criteri, di solito FCFS (*First Come First Served*). Si possono verificare delle perdite di celle qualora uno o più buffer saturino a causa del fenomeno dell'*Head Of Line blocking* (HOL) e cioè il blocco della coda di attesa, causato dalla cella che si trova in posizione di testa la quale è impossibilitata a raggiungere l'uscita desiderata.

19.4.2 Commutatori con buffer in uscita

I buffer sono associati ad ogni singola uscita del commutatore e vengono caricati, ad ogni ciclo di rete, con un determinato numero di celle selezionate tra quelle destinate alla corrispondente uscita. Se il numero di celle che si presentano agli ingressi e che sono destinate tutte alla stessa uscita è minore o uguale al limite prestabilito non si ha perdita, altrimenti è necessario attuare una selezione per eliminare le celle in esubero. Anche in questo caso occorre stabilire una politica di selezione facendo, ad esempio, passare le celle con la priorità più elevata.

Un tipico commutatore appartenente a questa classe è il *Knock-out switch* proposto da AT&T (figura 19.11). Esso consta di più bus di ingresso ai quali sono collegati un certo numero di blocchi di uscita. Questi blocchi sono costituiti da:

- filtri di cella *F*, che lasciano proseguire solo le celle indirizzate verso l'uscita cui i filtri appartengono;
- un concentratore (*knock-out concentrator)*, dal quale deriva la denominazione dell'intero commutatore che effettua la selezione delle celle;
- un buffer, nel quale vengono memorizzate le celle selezionate prima di essere avviate verso l'uscita.

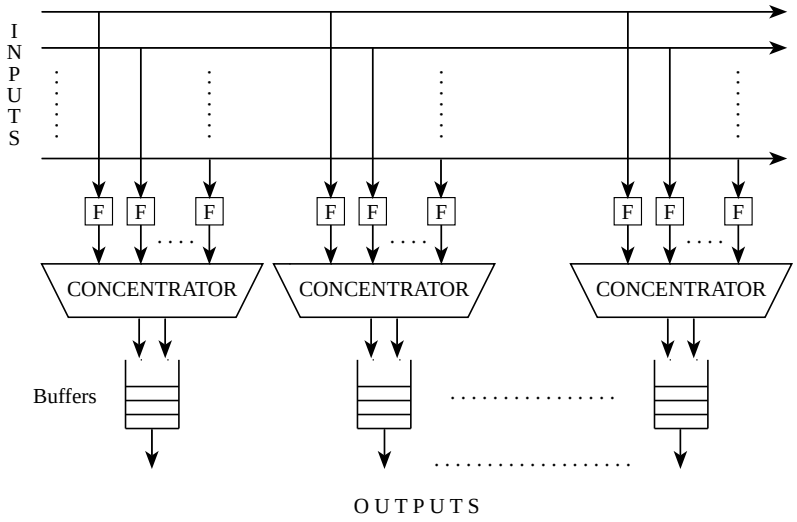


Fig. 19.11 - Knock-out switch.

19.4.3 Commutatori con buffer condiviso

Le strutture di commutazione appartenenti a questa classe dispongono di un'area di memorizzazione che è comune sia agli ingressi sia alle uscite. Un esempio di un tale sistema è il commutatore *Switch-on-a-chip* (figura 19.12), proposto da IBM.

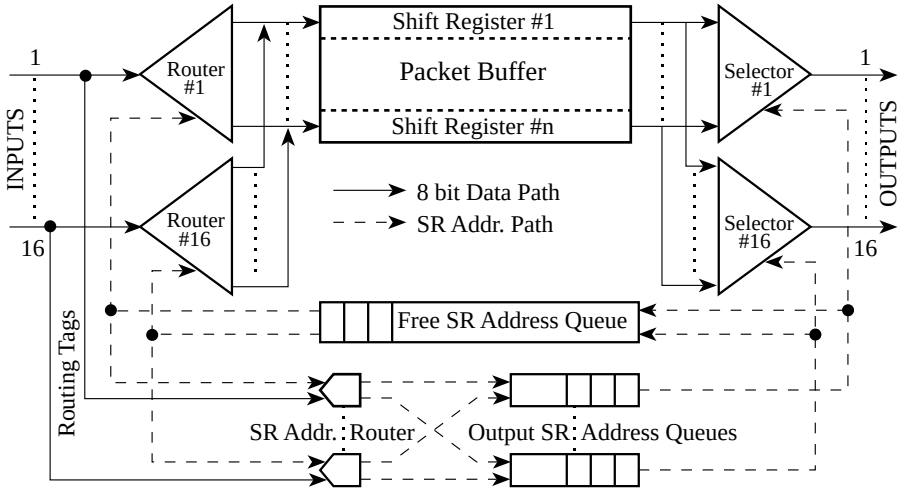


Fig. 19.12 - IBM Switch-on-a-chip.

Si tratta di un commutatore single-chip sviluppato dal laboratorio di ricerca IBM di Zurigo (clock a 50 MHz, 2.4 milioni di transistor, 472 pin di I/O). Le sue caratteristiche principali sono: una matrice di commutazione 16 x 16, velocità delle connessioni sino a 400 Mbps, capacità trasmissiva totale pari a 6.4 Gbps e possibilità di connettere più chip per realizzare una matrice con un maggior numero di porte.

Ogni cella in arrivo viene memorizzata nel buffer condiviso costituito da un banco di Shift Register (SR). All'ingresso, attraverso i router possono entrare fino a 16 celle contemporaneamente e analogamente, tramite i selector possono uscire fino a 16 celle contemporaneamente.

19.5 ASPETTI TRASMISSIVI

Come abbiamo già visto, la tecnica ATM può essere impiegata sia nelle reti di telecomunicazione pubbliche sia nelle reti locali e, conseguentemente, la UNI è stata specificata a livello fisico per poter operare con i diversi standard riportati in figura 19.13.

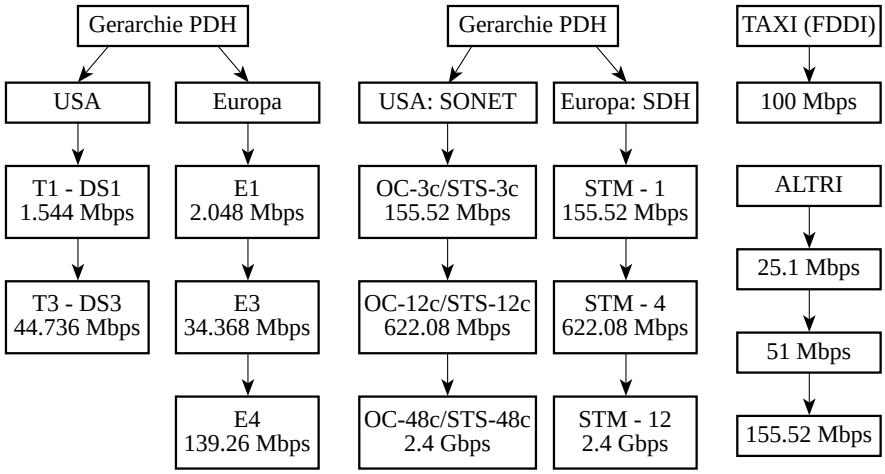


Fig. 19.13 - Standard a livello fisico.

Alcuni di questi prevedono di usare ATM in modo "nativo" sul canale trasmissivo e sono quindi idonei solo in ambito LAN. Tra questi evidenziamo il 25 Mb/s proposto da IBM, in grado di operare su cavo UTP di categoria 3 e accettato come standard dall'ATM Forum, il 51 Mb/s e il 155 Mb/s pensato quest'ultimo principalmente per la fibra ottica multimodale.

Sempre in ambito di rete locale esiste la possibilità di trasportare celle ATM usando il livello fisico di FDDI (interfaccia detta TAXI). Si noti come in questo caso, a causa della presenza della codifica 4B5B, non sia più possibile utilizzare l'HEC per correggere errori singoli, ma solo per rilevare errori di trasmissione.

Altri standard sono stati concepiti per utilizzare ATM in ambito geografico, incapsulando le celle nelle trame plesiocrone (PDH, si veda il paragrafo 12.5), oppure in quelle sincrone (SDH/SONET, si veda il paragrafo 12.6).

La gerarchia sincrona SDH/SONET dovrebbe soppiantare la precedente gerarchia plesiocrona PDH e gli standard nativi per fibra ottica e TAXI poiché:

- esistono ormai dei single-chip contenenti un trasmettitore/ricevitore SDH/SONET;
- SDH/SONET garantisce una ottima interoperabilità in ambienti multivendor, sia su base locale, sia su base geografica;
- SDH/SONET fornisce ottime funzionalità di gestione remota degli apparati di rete da parte di un centro di controllo.

19.6 ASPETTI DI PROTOCOLLO

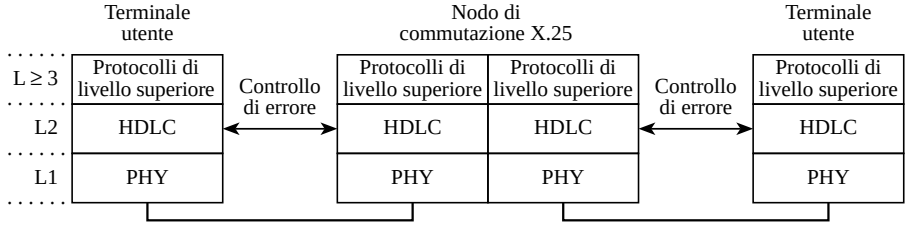
L'architettura dei protocolli ATM è stata ideata seguendo la filosofia *Core & Edge*, la quale prevede che le funzionalità di protocollo atte al trasporto di informazioni tra gli utenti della rete non siano implementate in modo paritetico in ogni punto attraversato dalla comunicazione [5]. Ciò implica che nei punti interni alla rete siano operativi solo i protocolli di livello più basso, i quali devono svolgere il minimo delle funzionalità necessarie al trasporto dell'informazione; nei punti terminali, invece, devono essere presenti, oltre ai precedenti, anche protocolli di livello superiore atti a fornire all'utenza ulteriori funzionalità per il trattamento di flussi informativi specifici.

Concettualmente la filosofia Core & Edge è profondamente diversa da quelle su cui si basano le reti a commutazione di pacchetto esistenti come, ad esempio, le reti X.25. Queste, per mantenere un elevato livello qualitativo della comunicazione end-to-end, nonostante l'infrastruttura trasmissiva inaffidabile per la quale erano state concepite, devono effettuare un controllo di errore su ogni collegamento fisico interno alla rete mediante un protocollo HDLC (si veda paragrafo 13.2 e la figura 19.14a). Questo fatto comporta un overhead computazionale che penalizza pesantemente le prestazioni della rete.

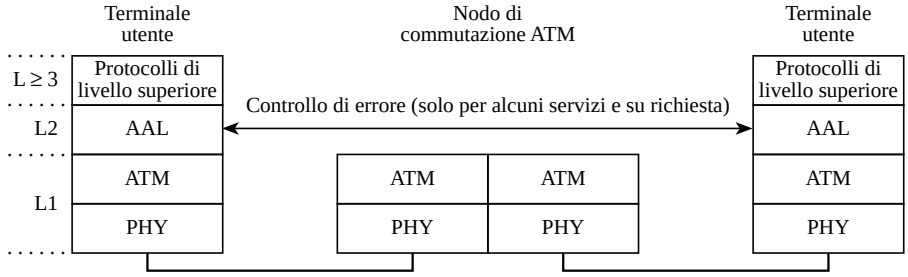
L'evoluzione dei mezzi trasmissivi, soprattutto nel campo delle fibre ottiche, ha ridotto drasticamente il tasso di errore all'interno della rete. Ciò ha consentito di demandare interamente il controllo degli errori agli estremi (Edge) della connessione, lasciando alla rete (Core) il solo compito di trasportare il bit stream utilizzando nodi

di commutazione dotati di protocolli di linea molto leggeri ed efficienti dal punto di vista computazionale (figura 19.14b). Questa suddivisione di compiti ha condotto ad una notevole semplificazione architetturale, la cui principale conseguenza è stato un incremento significativo nelle prestazioni della rete.

La figura 19.15 mostra il *Protocol Reference Model* (PRM) raccomandato da CCITT per ATM, nell'ambito del progetto B-ISDN.



a: Rete a pacchetto X.25: Controllo di errore su ogni link interno alla rete.



b: Rete ATM (B-ISDN): Controllo di errore end-to-end.

Fig. 19.14 - Confronto tra le architetture di rete X.25 e ATM.

Si può notare un'architettura stratificata simile a quella del modello di riferimento OSI, ma, a differenza di questo, si ha anche uno sviluppo tridimensionale dovuto alla suddivisione dei protocolli su tre piani:

1) uno *User Plane*, atto al trasporto delle informazioni d'utente, quali fonia, video e dati;
2) un *Control Plane* che si occupa del trasporto e del trattamento dell'informazione di segnalazione;
3) un *Management Plane* che è strutturato in:
   - un *Layer Management Subplane*, il cui scopo è la gestione dei flussi informativi di OAM (Operation And Maintenance, configurazione e manutenzione della rete) e dei canali di segnalazione;

- un *Plane Management Subplane*, che riveste le funzioni di coordinamento tra i piani precedenti e supervisione a livello locale del sistema.

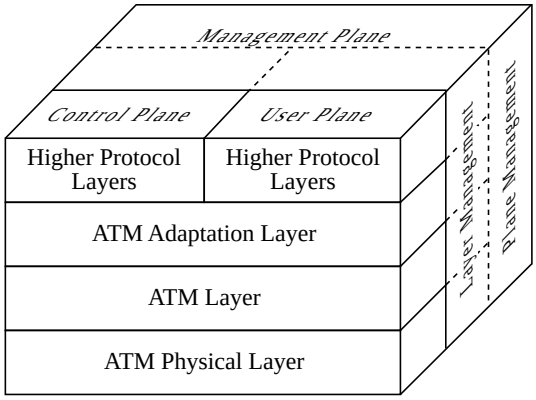


Fig. 19.15 - B-ISDN Protocol Reference Model.

Ogni piano, eccetto il Management Plane, è a sua volta suddiviso su tre livelli (figura 19.16): *Physical Layer*, *ATM Layer* e *ATM Adaptation Layer*.

<table>
<tr><td>Convergence sublayer</td><td colspan="2" rowspan="2">ATM Adaptation Layer</td></tr>
<tr><td>Segmentation and reassembly</td></tr>
<tr><td>Cell header generation/extraction</td><td colspan="2" rowspan="3">ATM Layer</td></tr>
<tr><td>Cell VCI/VPI translation</td></tr>
<tr><td>Cell MUX/DEMUX</td></tr>
<tr><td>Cell rate decoupling</td><td rowspan="4">Transmission Convergence</td><td rowspan="6">Physical Layer</td></tr>
<tr><td>HEC generation/verification</td></tr>
<tr><td>Cell delineation</td></tr>
<tr><td>Transmission frame generation</td></tr>
<tr><td>Bit timing</td><td rowspan="2">Physical Medium Dependent</td></tr>
<tr><td>Bit TX/RX</td></tr>
</table>

Fig. 19.16 - Suddivisione in livelli e sottolivelli dei piani del PRM.

19.7 PHYSICAL LAYER

Il livello fisico isola e rende indipendente il livello ATM dal particolare sistema trasmissivo adottato. Esso è costituito da due sottolivelli: il *Physical Medium Dependent* (PMD) ed il *Transmission Convergence* (TC). Come indica chiaramente il nome, il PMD dipende strettamente dal particolare portante fisico adottato (doppino, cavo coassiale, fibra ottica) e la sua funzione è quella di trasmettere/ricevere i bit di informazione ed i segnali di sincronismo sul canale.

Il compito del TC è invece quello di generare la trama da inviare in linea (*transmission frame generation*) ed inserirvi le celle che gli passa il livello ATM soprastante. In ricezione deve riconoscere i confini delle celle (*cell delineation*) all'interno della trama ed estrarle. Un altro compito del TC è quello di adattare il flusso di celle ricevute dal livello ATM alla capacità netta del suddetto frame (*cell rate decoupling*) inserendo (ed estraendo in ricezione) opportune celle vuote. Deve infine generare/verificare il campo HEC presente nello header delle celle (*HEC generation/verification*).

19.8 ATM LAYER

Il livello ATM si occupa dell'instradamento e del (de)multiplexing delle celle sulle connessioni virtuali. Come si è visto in precedenza, questa funzione viene svolta con cambio di multiplex (*cell mux/demux)* ed un cambio di etichetta (*cell VCI/VPI translation*) da parte dei nodi di commutazione attraversati dalla connessione. Un'altra funzione del livello ATM è quella di generare/estrarre l'intestazione per le celle in partenza/arrivo (*cell header generation/extraction*).

Il livello ATM può essere collocato nell'ambito del modello di riferimento OSI al livello Fisico (figura 19.17): un canale virtuale tra due terminazioni della rete ATM è esattamente analogo ad un collegamento fisico, è un *cavo virtuale* che trasporta un flusso di bit senza effettuare alcun controllo su di essi.

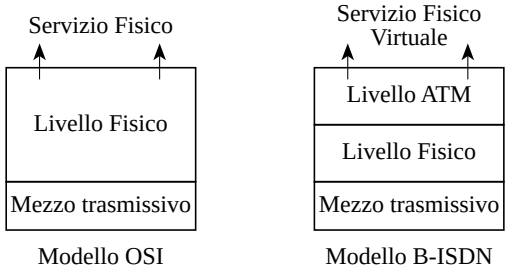


Fig. 19.17 - Modelli B-ISDN ed OSI: il Servizio Fisico.

Un circuito virtuale ATM non è però pienamente assimilabile ad un collegamento fisico punto-punto per due motivi. In primo luogo, la rete ATM può realizzare tra due terminazioni d'utente un qualunque numero di connessioni virtuali fino alla saturazione delle linee di interfaccia UNI; inoltre ad ogni punto di accesso alla rete ATM, corrispondente all'interfaccia UNI, possono essere collegati un certo numero di terminali utente che condividono tale interfaccia per formare la cosiddetta *Customer Premises Network* (CPN) (figura 19.18).

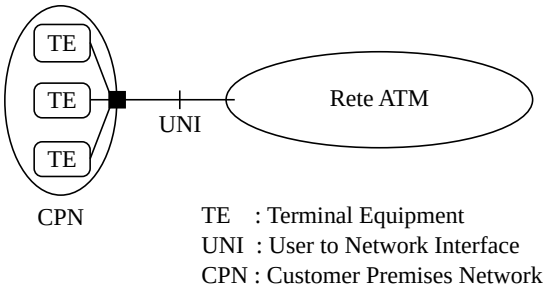


Fig. 19.18 - Customer Premises Network.

Questo fatto è ovvio se si pensa che lo scopo di B-ISDN è quello di fornire una serie di servizi integrati che sono fruibili tramite un unico punto di collegamento utilizzando diversi tipi di terminali (televisori, telefoni, calcolatori), almeno fino a quando non saranno disponibili terminali multimediali.

19.9 ATM ADAPTATION LAYER (AAL)

Il servizio di trasporto di celle offerto dal livello ATM è di un ordine talmente basso da essere praticamente inutilizzabile dalla maggior parte delle applicazioni. Per questo motivo è stato introdotto un livello di adattamento ATM (*AAL: ATM Adaptation Layer*) il quale è in grado di fornire una certa classe di servizi attivabili in base alle esigenze dell'utenza. CCITT ha definito quattro classi di servizio come mostrato in figura 19.19.

La classificazione dei servizi avviene tenendo conto di tre parametri:

- riferimento temporale tra sorgente e destinazione;
- bit rate;
- modalità di connessione.

Nella classe A si ha un riferimento temporale tra sorgente e destinazione, il bit rate è costante ed il servizio è connection oriented: essa risulta particolarmente

adatta per la telefonia numerica con codifica PCM a 64 Kb/s oppure all'interconnessione trasparente di canali numerici di tipo T1 o E1*. Per questo motivo tale classe di servizio è anche denominata *emulazione di circuito*.

	CLASSE A	CLASSE B	CLASSE C	CLASSE D
Riferimento temporale tra sorgente e destinazione	Necessario		Non necessario	
Bit rate	Costante (CBR)	Variabile (VBR)		
Modalità di connessione	Connection oriented			Connectionless

Fig. 19.19 - Classi di servizio offerte da AAL.

La classe B si differenzia dalla precedente per via del bit rate, che in questo caso è variabile. Viene usata per il trasporto di audio e video numerico generati mediante codec a bit rate variabile.

La classe C perde il riferimento temporale tra sorgente e destinazione e pertanto non è più adatta ad applicazioni real time. Offrendo un servizio connection oriented, viene usata per trasferimenti dati a pacchetto tipo X.25 sul piano utente o per attività di segnalazione sul piano di controllo.

Esiste infine la classe D che offre un servizio connectionless, privo di riferimenti temporali e con bit rate variabile. Essa è adatta al trasporto del traffico dati di tipo datagram, caratteristico delle LAN.

Per implementare le classi di servizio precedenti CCITT ha definito tre tipi di AAL: tipo 1 per la classe A, tipo 2 per la classe B e tipo 3/4 per le classi C e D. È stato anche proposto da parte dell'ATM Forum l'AAL di tipo 5, denominato ufficiosamente *Simple and Efficient Adaptation Layer* (SEAL), che è una semplificazione del tipo 3/4 atta a rendere il protocollo più efficiente e, di conseguenza, più adatto ad un impiego nelle LAN ATM.

Tutti i tipi di AAL sono suddivisi in due sottolivelli: *Segmentation And Reassembling* (SAR) e *Convergence Sublayer* (CS). SAR si occupa di segmentare le PDU (*Protocol Data Unit*) provenienti dai livelli superiori in celle ATM e viceversa, mentre CS svolge delle funzioni particolari a seconda della classe di servizio implementata.

Dal momento che in questa sede si è interessati alle problematiche di interconnessione di LAN mediante reti ATM, è opportuno soffermarsi con maggior attenzione sui servizi di trasporto dati offerti da AAL3/4 e da AAL5 [2].

---

* T1 è l'elemento base della gerarchia di multiplazione PDH statunitense e corrisponde a 1.5 Mb/s. E1 (2 Mb/s) è il suo equivalente europeo (si veda il paragrafo 12.5).

19.9.1 AAL tipo 3/4

AAL tipo 3/4 è molto simile al livello MAC dello standard IEEE 802.6 per le MAN, noto anche come DQDB (*Distributed Queue Dual Bus*), discusso nel capitolo 9. Questa rassomiglianza è sottolineata dal fatto che la SAR-PDU* di AAL 3/4 e la MAC-PDU di DQDB sono identiche (si vedano le figure 19.20 e 9.14).

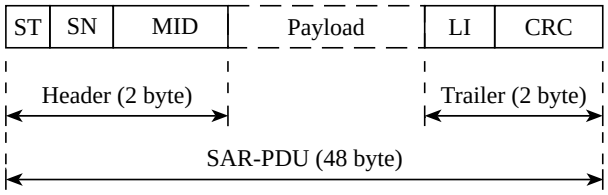


Fig. 19.20 - Formato della SAR-PDU di AAL tipo 3/4.

Il significato dei campi della SAR-PDU è il seguente:

- ST (*Segment Type*, 2 bit): specifica a quale sezione del messaggio (CS-PDU) corrisponde una SAR-PDU. I valori possibili di ST sono:
  - BOM (*Beginning Of Message*),
  - COM (*Continuation Of Message*),
  - EOM (*End Of Message*),
  - SSM (*Single Segment Message*);
- SN (*Sequence Number*, 4 bit): indica qual è la posizione di un segmento di tipo COM all'interno del messaggio, con numerazione modulo 16;
- MID (*Message IDentifier*, 10 bit): stabilisce a quale messaggio appartiene un determinato segmento; utilizzato per multiplare più CS-PDU su una sola connessione virtuale;
- PAYLOAD: campo dati lungo 44 byte;
- LI (*Length Indicator*, 6 bit): viene usato per stabilire la lunghezza effettiva del payload qualora sia necessario effettuare il *padding* in una SAR-PDU di tipo EOM o SSM;
- CRC (*Cyclic Redundancy Code*, 10 bit): codice per il controllo degli errori; copre tutta la SAR-PDU.

* Ai fini di una più agevole comprensione delle definizioni date nel seguito, in figura 19.21 è stata riportata la terminologia B-ISDN per quanto concerne la denominazione delle unità dati di protocollo.

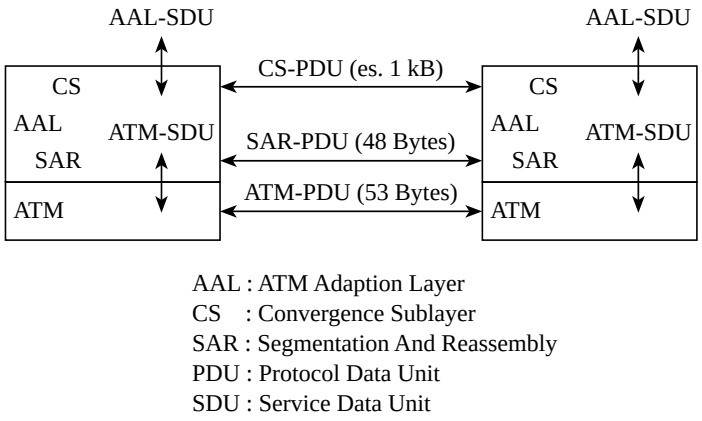


Fig. 19.21 - Terminologia nel modello di riferimento B-ISDN.

Il trasferimento delle AAL-SDU può avvenire nei seguenti modi (figura 19.21):

- se le AAL-SDU sono molto brevi (ad esempio se trasportano i caratteri digitati da un utente durante una sessione remota con un host) possono essere accorpate in un'unica CS-PDU (*blocking/deblocking*);
- se invece sono molto lunghe (ad esempio blocchi di 64 KByte derivanti da una operazione di file transfer) vengono suddivise in una o più CS-PDU (*segmentation/reassembling*).

Il sottolivello SAR dell'entità AAL in trasmissione deve:

- segmentare una CS-PDU in una sequenza di SAR-PDU del tipo BOM-COM...COM-EOM (oppure una singola SSM se la CS-PDU è molto breve);
- assegnare il corretto valore di SN e calcolare il CRC per ogni segmento;
- multiplare, se necessario, più CS-PDU, contraddistinguendo le varie sequenze di SAR-PDU ottenute con valori di MID diversi.

I compiti del sottolivello SAR della entità AAL in ricezione sono:

- verificare il CRC di tutte le PDU ricevute;
- assemblare una CS-PDU raggruppando tutti i segmenti con lo stesso MID, verificandone la completezza attraverso numeri di sequenza ed il campo ST;
- passare al livello CS tutte le CS-PDU riassemblate correttamente e scartare quelle incomplete o con segmenti corrotti.

Il sottolivello CS ha invece il compito di gestire le comunicazioni in modo connectionless (Classe D) e connection oriented (Classe C), effettuando:

- mapping tra AAL-SAP (utente del livello AAL) e le connessioni virtuali;
- accorpamento/separazione di AAL-SDU di piccole dimensioni oppure segmentazione/riassemblaggio di AAL-SDU di grosse dimensioni;
- gestione dei buffer di ricezione/trasmissione;
- controllo di errore sulle CS-PDU, con eventuale richiesta di ritrasmissione se si opera in classe C (modalità connection oriented).

Da quanto sopra esposto è evidente che il sottolivello CS di AAL 3/4 consente di disaccoppiare le AAL-SDU, cioè i blocchi di informazione passati dai livelli di protocollo superiori (ad es. IP, XNS, IPX), dalle SAR-PDU.

I servizi offerti da AAL 3/4 sono orientati unicamente al trasferimento di AAL-SDU e sono accessibili tramite due primitive:

- AAL-UNITDATA-REQ: è la primitiva mediante la quale un livello superiore richiede all'entità AAL locale di trasferire una AAL-SDU all'entità o alle entità AAL remota/e;
- AAL-UNITDATA-IND: è la primitiva che indica al livello superiore dell'entità AAL locale che è giunta una AAL-SDU dall'entità AAL remota.

A seconda della classe di servizio richiesta ad AAL si hanno i seguenti modi operativi:

- *Operazioni non sicure* (Classe D): le AAL-SDU possono essere perse o danneggiate in quanto non si effettua alcun controllo sulle CS-PDU;
- *Operazioni sicure* (Classe C): le AAL-SDU sono trasferite con garanzia di consegna e correttezza dei dati, dato che le CS-PDU perse o danneggiate vengono ritrasmesse; esiste anche una forma di controllo del flusso. Queste operazioni consentono di realizzare, con un intrinseco degrado del throughput, delle connessioni ATM end-to-end assolutamente error-free. In genere si preferisce però non usare questa modalità operativa e demandare il controllo di errore e flusso ad un protocollo di trasporto di livello superiore, dal momento che una rete ATM è in grado di fornire un servizio dalla qualità estremamente elevata (BER: Bit Error Rate $\sim 10^{-8}$).

Alla luce di quanto è stato detto finora sul livello AAL tipo 3/4, risulta chiaro (figura 19.22) che esso è equivalente al livello Data Link del modello OSI. CCITT ha addirittura raccomandato che il servizio di classe C offerto da AAL tipo 3/4 sia compatibile con HDLC.

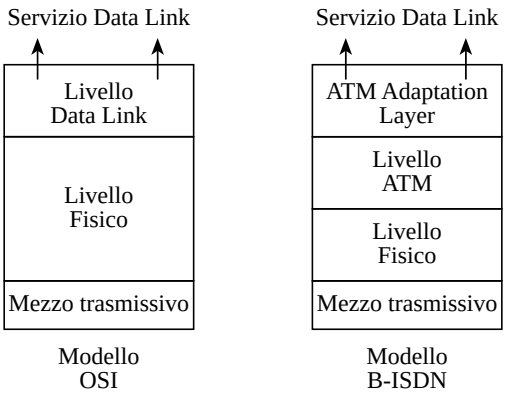


Fig. 19.22 - Modelli B-ISDN ed OSI: il Servizio Data Link.

19.9.2 AAL tipo 5

Dopo aver analizzato le caratteristiche fondamentali di AAL tipo 3/4 è facile rendersi conto che si tratta di un livello di protocollo decisamente pesante dal punto di vista computazionale. Per questo motivo ATM Forum ha proposto SEAL (*Simple and Efficent Adaptation Layer*), ratificato successivamente da CCITT come AAL tipo 5.

Come risulta evidente dal nome, SEAL è una semplificazione di AAL 3/4 che tende a renderlo più efficiente. Il guadagno in efficienza va però a scapito della robustezza del protocollo: questo tipo di AAL è in grado di offrire soltanto un servizio non connesso.

La semplificazione è molto drastica, sia per quanto concerne il sottolivello CS che è stato praticamente svuotato, sia per quanto riguarda il sottolivello SAR. La SAR-PDU, riportata in figura 19.23, è lunga 48 byte e coincide con il payload della cella ATM. Una CS-PDU viene suddivisa in una sequenza di segmenti di 48 byte che non sono né numerati né identificati in alcun modo. L'ultimo segmento, oltre ad un eventuale riempimento per normalizzare la lunghezza a 40 byte, contiene anche il CRC a 32 bit calcolato sull'intera CS-PDU e un campo CTRL/Length su 4 byte. Questo segmento viene contraddistinto dal settaggio ad 1 del bit PT (*Payload Type*) dell'intestazione della cella ATM.

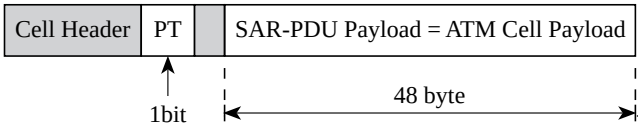


Fig. 19.23 - Formato della SAR-PDU di AAL tipo 5.

Quando al sottolivello SAR dell'entità AAL 5 in ricezione giunge una cella con PT settato, essa assembla tutte le SAR-PDU estratte in precedenza in una CS-PDU, aggiunge al tutto l'ultimo segmento e verifica la length e il CRC (figura 19.24). Se la CS-PDU è valida viene restituita al livello CS, altrimenti viene scartata senza ulteriori provvedimenti, esattamente come una trama del livello MAC di Ethernet.

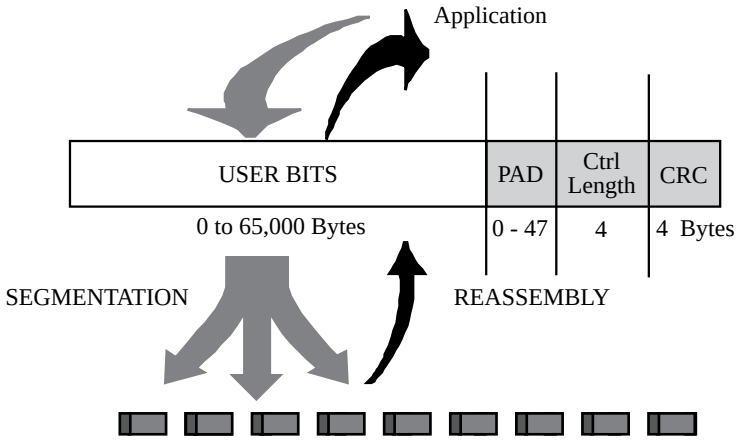


Fig. 19.24 - Processo di segmentazione e riassemblaggio in AAL tipo 5.

19.10 ASPETTI DI SEGNALAZIONE

La segnalazione serve ad attivare e disattivare le connessioni virtuali stabilendone il tipo: punto-punto o punto-multipunto. La segnalazione deve anche fornire la negoziazione della classe di servizio desiderata, con la relativa QoS, e dei parametri del traffico offerto, sia in fase di apertura delle connessioni, sia in fase di riconfigurazione durante il corso di una chiamata.

Si distinguono due tipi di segnalazione: la *segnalazione di accesso,* usata dalle terminazioni d'utente per richiedere l'attivazione di connessioni virtuali, e la *segnalazione in rete*, usata per propagare sulla rete tali richieste. La segnalazione di accesso viene trasferita su una connessione virtuale tra terminale e nodo di commutazione. Tale connessione virtuale viene creata tramite una operazione di*metasegnalazione* su un VPI/VCI riservato. Una volta aperta la connessione per la segnalazione, vengono attivate le suddette procedure di negoziazione dei parametri di comunicazione.

I sistemi di segnalazione attualmente adottati sulle reti ATM sono descritti nello standard CCITT Q.93B. Questo deriva dallo standard Q.931 impiegato su ISDN che si basa sul protocollo di segnalazione a canale comune *Signaling System Number 7*

(SSN7) sviluppato da BellCore.

La figura 19.25 mostra i messaggi scambiati su una rete per l'instaurazione di una connessione.

La figura 19.26 mostra i messaggi scambiati su una rete per l'abbattimento di una connessione.

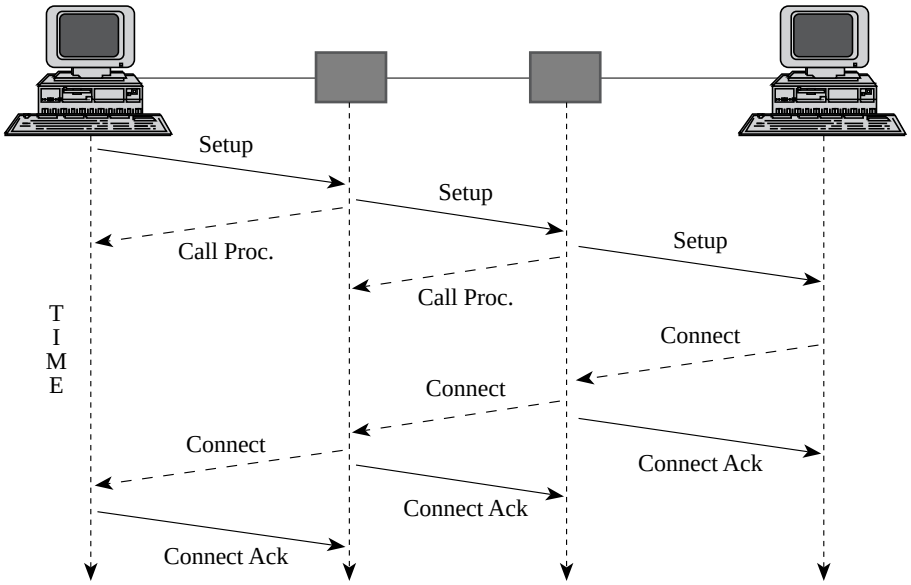


Fig. 19.25 - Segnalazione per "Call Setup".

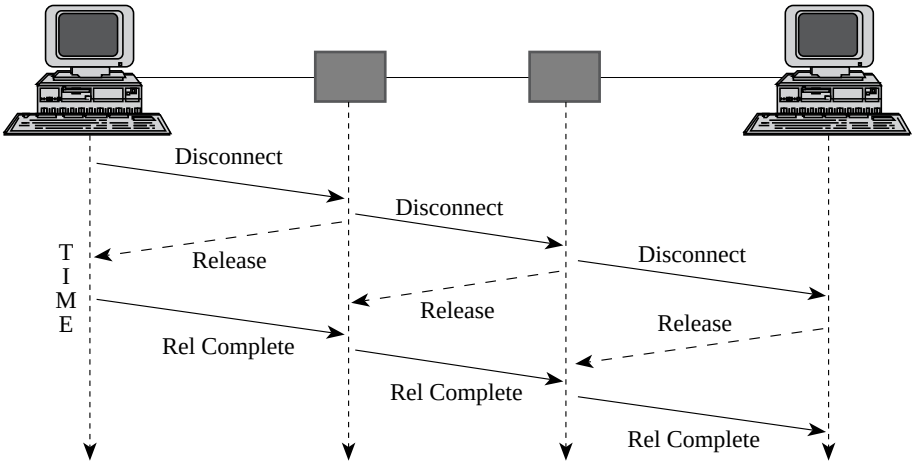


Fig. 19.26 - Segnalazione per "Call Clear".

19.12 ASPETTI DI TRAFFICO

Si è accennato in precedenza che le reti ATM devono essere in grado di gestire flussi informativi aventi caratteristiche molto differenti. In generale si può caratterizzare il traffico in base alla banda richiesta ed alla continuità (flusso di dati continuo oppure a burst). È pertanto necessario dotare la rete di robuste e, contemporaneamente, efficienti procedure di controllo del flusso al fine di assicurarne un corretto funzionamento in qualunque condizione di carico.

Queste procedure operano su due livelli distinti: a livello di chiamata, accettando o respingendo le chiamate a seconda delle risorse disponibili, ed a livello di interfaccia UNI, controllando effettivamente il flusso di traffico inviato dall'utente (operazione detta *policing*).

19.12.1 Accettazione della connessione

Nelle reti telefoniche classiche una connessione viene rifiutata qualora tutti i circuiti fisici tra i due estremi interessati dalla comunicazione siano occupati. Allo stesso modo una rete ATM tende a rifiutare le chiamate per le quali non è possibile trovare un circuito virtuale su cui instradarle oppure se una loro eventuale accettazione causa un degrado inaccettabile delle prestazioni delle connessioni già instradate.

Di conseguenza, l'accettazione di una nuova connessione dipende sia dalla sua occupazione di banda, sia dalle risorse di rete ancora libere. Affinché la rete possa effettuare le verifiche precedenti è necessario che l'utente chiamante fornisca una descrizione dettagliata del traffico che ha intenzione di richiedere in termini di:

- banda di picco;
- banda media;
- fattore di *burstiness* (rapporto tra le due bande precedenti nell'ordine di elencazione);
- durata media dei burst.

In base a questi parametri la rete riesce a stabilire se ha ancora banda sufficiente per instradare la nuova chiamata e, in caso affermativo, se il traffico generato dalla nuova connessione non va ad inficiare quello delle altre già stabilite a causa, ad esempio, di burst troppo lunghi con banda di picco elevata.

La stazione di utente, una volta stabilta la connessione, dovrà rispettare i parametri di traffico pattuiti, dotandosi di un modulo di *shaping* in grado di spaziare le celle prima di trasmetterle in modo che non violino il contratto. Ad esempio, se la stazione ha aperto una connessione per trasferire dati a 2 Mb/s su un canale a 155 Mb/s e si trova

a dover trasmettere un pacchetto IP di 4KB, dopo averlo frammentato in celle, dovrà distanziare temporalmente la trasmissione delle stesse, generando quindi un flusso a 2 Mb/s e non trasmetterle una dietro l'altra generando un flusso a 155 Mb/s.

19.12.2 Controllo dei parametri utente

Nelle reti a commutazione di pacchetto di tipo convenzionale il flusso del traffico viene controllato mediante protocolli a finestra che, essendo di tipo *reattivo*, comportano un overhead inaccettabile per le applicazioni real time come la videoconferenza. Per questo motivo nelle reti ATM si adottano meccanismi di tipo *preventivo* basati sulla verifica che i parametri del traffico offerto su ogni connessione siano conformi a quelli dichiarati dall'utente all'atto dell'instaurazione della stessa.

Il metodo più utilizzato per il controllo dei parametri utente è il *Leaky Bucket* (scolapasta). La rete associa ad ogni connessione un contatore che incrementa al ricevimento di una cella e decrementa con frequenza costante, calcolata in base ai parametri dichiarati all'inizializzazione. Se il conteggio eccede una soglia prefissata, calcolata come sopra, allora la rete scarta tutte le celle provenienti dalla connessione associata al contatore in overflow fino a quando questo non sia tornato sotto il livello di guardia.

BIBLIOGRAFIA

[1] William Stalling, "ISDN and Broadband ISDN", MacMillam Publishing Company, New York, 1992.

[2] TA-NWT-001113: "Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements", Bellcore, Issue 1, August 1992.

[3] S. Giorcelli: "La Tecnica ATM nelle Reti ad Alta Velocità", CSELT, 1991.

[4] The ATM Forum: "ATM: User-Network Interface Specification V 3.0", Prentice-Hall, 1993.

[5] M. De Prycker, R. Peschi, T. Van Landegem: "B-ISDN and the OSI Protocol Reference Model", IEEE Network Magazine, March 1993.

[6] Colella, E. Gardner, R. Callon, "RFC 1237: Guidlines for OSI NSAP Allocation in the Internet", 07/23/1991.

[7] Autori vari, "Issues and Challanges in ATM Networks", Communications of the ACM, Vol. 38, No. 2, February 1995.

20

LE LAN IN TECNOLOGIA ATM

Nel capitolo 11 abbiamo trattato l'evoluzione delle LAN e abbiamo visto come una LAN odierna si basi sempre su un cablaggio strutturato, con topologia stellare, in cui le stazioni sono collegate da canali punto-punto con degli switch, e questi tra di loro per formare una rete fisica su cui si possono definire delle reti locali virtuali. Già in quel capitolo abbiamo accennato alla possibilità di utilizzare la tecnologia ATM per la realizzazione delle dorsali, ma ATM può essere usato anche come una tecnologia per realizzare reti locali (LAN ATM) che si integrano con quelle tradizionali e mirano a sostituirle.

In particolare, le LAN ATM si imporranno prima in quei settori che richiedono applicazioni a larga banda con qualità del servizio garantita, quali il desktop-video e le comunicazioni multimediali, dove le LAN tradizionali soffrono di una serie di problemi e di limitazioni che le rendono inadatte; quindi si proporranno come una alternativa alle LAN classiche, caratterizzate da un miglior rapporto prestazioni/prezzo.

L'attenzione che l'industria informatica pone sulle LAN ATM è notevole, come testimonia il fatto che sul mercato sono già presenti prodotti per realizzare LAN ATM. I primi settori di applicazione delle LAN ATM possono essere così schematizzati:

- realizzazione di dorsali veloci e multimediali;
- interconnessione di sistemi multimediali in grado di gestire dati, suono e immagini in movimento;
- interconnessione di workstation per realizzare architetture di calcolo distribuito ad alte prestazioni;
- interconnessione di sistemi grafici che richiedono un accesso veloce a grandi archivi di immagini: per esempio, sistemi per la gestione della cartografia.

Inoltre la necessità di far crescere le prestazioni delle LAN tramite l'introduzione della tecnologia ATM è anche giustificata dalla sempre crescente potenza di calcolo dei processori: una relazione tra questa, espressa in MIPS (*Millions Instructions Per Second*) e la velocità espressa in Mb/s è schematizzata in figura 20.1.

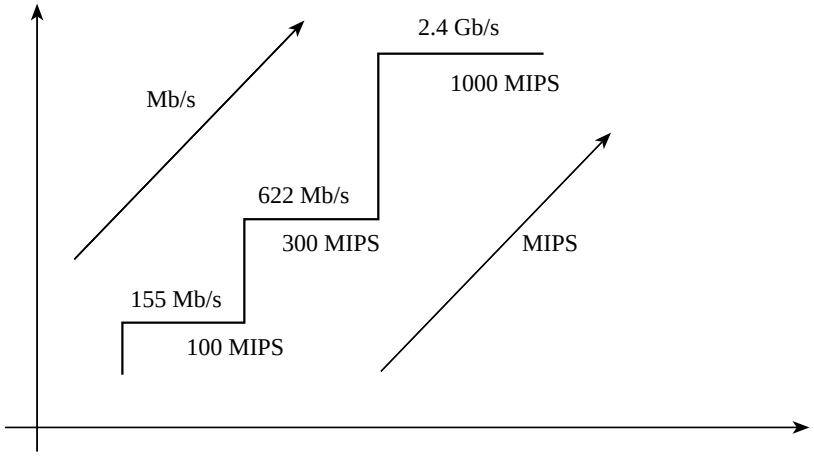


Fig. 20.1 - Relazione tra potenza di calcolo e velocità trasmissive.

Il problema più significativo da risolvere per utilizzare la tecnologia ATM nella realizzazione delle LAN è che ATM non è stato concepito nell'ambito del progetto IEEE 802 e differisce in parecchi aspetti significativi dalle LAN basate su tecnologie tradizionali.

20.1 CONFRONTO TRA LE LAN CLASSICHE E LE LAN ATM

Le reti locali classiche nascono come "reti ad accesso condiviso", cioè reti in cui tutte le stazioni condividono un unico canale trasmissivo (si veda il paragrafo 5.1). L'evoluzione delle LAN classiche con l'introduzione degli switch (si veda il paragrafo 11.3) supera in parte questo limite garantendo ad ogni stazione un collegamento punto-punto verso la rete, che però è di tipo half-duplex (trasmissione monodirezionale ad un dato istante di tempo) ed è soggetto a condivisione con il traffico di multicast/broadcast. Inoltre lo switch non ha meccanismi per allocare risorse alle singole stazioni e questo non permette nelle LAN classiche di realizzare meccanismi di trasmissione a *banda garantita*, possibili su ATM e necessari per il traffico di tipo multimediale.

Le reti locali classiche hanno un livello MAC non connesso. Quando una stazione deve trasmettere un pacchetto lo fa direttamente specificando unicamente gli indirizzi MAC di mittente e destinatario, senza stabilire alcuna connessione: la rete fa il massimo sforzo per consegnare il pacchetto al destinatario, ma non garantisce nè la consegna, nè il ritardo massimo. ATM è una tecnologia che richiede la presenza di connessioni: una stazione ATM prima di trasferire una cella deve aprire una connessione con la stazione di destinazione; la connessione ha certi parametri di qualità associati che richiedono l'allocazione di risorse dedicate sui nodi; la trasmissione avviene nel rispetto dei parametri di qualità associati; quando la stazione non intende più utilizzare la connessione deve chiuderla esplicitamente per rilasciare le risorse allocate sui nodi.

Nelle LAN classiche i dati sono trasmessi sotto forma di pacchetti aventi dimensioni variabili. Se la rete è estesa non è possibile prevedere il ritardo totale (latenza) subito da un pacchetto durante il transito nella rete. La variabilità della latenza non crea particolari problemi ai flussi di dati, ma può rendere incomprensibili voce ed immagini digitalizzate a causa del rumore che introduce. Nelle reti ATM il problema della variabilità della latenza viene drasticamente ridimensionato utilizzando le celle che sono unità di trasporto dati, di dimensioni piccole e fisse.

Nelle reti locali classiche la trasmissione dell'informazione avviene a livello fisico in modalità broadcast. Questo ha una implicazione a livello di sicurezza dei dati, dal momento che questi vengono propagati oltre che alla stazione destinataria anche a tutte le altre, ma sopprattutto consente di realizzare in modo estremamente semplice la trasmissione di pacchetti a tutte le stazioni (broadcast) o a gruppi di stazioni (multicast). Tale peculiarità è stata sfruttata nella realizzazione di tutti i protocolli di livello superiore (IP, DECnet, OSI, Novell, ...) che utilizzano pacchetti di multicast/broadcast di solicitation o advertisement (si veda il paragrafo 5.6.7) per tutte le attività di gestione del protocollo stesso. Per la sua natura connessa ATM non offre un analogo supporto per la trasmissione dei pacchetti multicast/broadcast.

Nelle reti locali classiche la capacità del mezzo trasmissivo e il protocollo MAC utilizzato sono tra di loro strettamente vincolati (si veda ad esempio, nel capitolo 6, come l'estensione massima di una rete Ethernet sia legata alla velocità di 10 Mb/s). Ciò implica l'impossibilità di incrementare le prestazioni della rete traendo vantaggio dai progressi tecnologici, se non al costo della sostituzione dell'intera rete (assenza di scalabilità). La tecnica ATM invece presenta delle possibilità di crescita prestazionali praticamente illimitate: se la tecnologia è in grado di realizzare collegamenti fisici e commutatori più veloci, la capacità trasmissiva della rete ne beneficia. I commutatori attualmente disponibili sono in grado di gestire linee operanti a 155 Mb/s, ma sono già in fase di prototipazione commutatori con linee a 622 Mb/s e 2.5 Gb/s.

A fronte di queste differenze l'utilizzo della tecnologia ATM nelle reti locali può avvenire in due modi diversi:

- sviluppando uno strato software da appoggiare su ATM per emulare il comportamento delle reti locali IEEE 802 e quindi non richiedendo alcuna modifica ai protocolli di più alto livello;
- andando a modificare i protocolli di più alto livello adattandoli a funzionare in modo nativo su ATM mediante interazione diretta con le ATM/API (Application Programming Interface).

Il primo approccio è quello proposto dall'ATM Forum con il nome di LAN Emulation e verrà descritto dettagliatamente nel paragrafo 20.4. Il secondo approccio è possibile per i protocolli principali ed in particolare vedremo nel capitolo 21 le modifiche che vengono proposte per adattare IP ad ATM.

20.2 REQUISITI DI UNA LAN ATM

Da una LAN ATM gli utenti e gli amministratori di sistema si aspettano almeno le stesse prestazioni e gli stessi servizi offerti dalle LAN convenzionali. Più precisamente:

- Interoperabilità con le reti esistenti: può essere raggiunta installando interfacce ATM all'interno di unità di internetworking quali gateway, router o bridge; oppure integrando nei commutatori ATM interfacce di rete locale classiche;
- Supporto trasparente dei protocolli esistenti: tutti i protocolli pensati per operare su una LAN appartenente al progetto IEEE 802 devono poter operare senza modifiche sulle LAN ATM, non solo i più importanti quali IP o OSI;
- Supporto dei protocolli di management: tutti gli apparati ATM devono essere dotati di agenti SNMP (*Simple Network Management Protocol*), che consentano il controllo remoto dello stato delle linee, dei commutatori e delle interfacce ATM nonché la raccolta di informazioni di tipo statistico e prestazionale;
- Facilità di installazione e configurazione: deve essere possibile, ad esempio, collegare o scollegare una stazione senza alcun intervento di ordine amministrativo;
- Robustezza e affidabilità: fintantoché esiste un percorso fisico tra due stazioni queste devono poter comunicare;
- Efficienza: se ci sono più percorsi fisici tra due stazioni, questi devono essere completamente saturati prima di rifiutare ulteriori richieste di connessione.

Se tutti questi requisiti sono soddisfatti, allora la LAN ATM può costituire un valido sostituto per la LAN esistente. Oltre al fatto che tutto continua a funzionare come in precedenza, si ottiene un significativo incremento del livello prestazionale dovuto alla maggior banda ed efficienza nel suo sfruttamento da parte della tecnica ATM.

Da una LAN ATM ci si attende inoltre:

- Supporto di una molteplicità di classi di servizio, come ad esempio la modalità connessa, real time ad elevato bit rate adatta al trasporto di un canale video da integrare in applicazioni multimediali;
- Possibilità di gestire connessioni multicast a larga banda (supportate cioè dall'hardware). Questo è un punto debole delle tecniche a commutazione di pacchetto: mentre nelle LAN classiche il multicasting è intrinseco nella tecnologia adottata, nelle LAN ATM deve essere fornito da hardware/ software addizionale;
- Offerta di una *Application Programming Interface* (API) che consenta lo sviluppo di applicazioni specifiche per ATM mediante l'interazione diretta con i vari AAL (ATM Adaption Layer), oppure interagendo direttamente in *raw mode* con il livello ATM.

Una LAN ATM che soddisfi i precedenti requisiti è in grado di fornire supporto ai servizi a larga banda, come il desktop video o le comunicazioni multimediali, sfruttando al massimo le risorse di rete e senza creare interferenze con le applicazioni meno sofisticate che "credono" di funzionare su una normale LAN.

20.3 ADOZIONE DI ATM NELLE LAN

L'introduzione della tecnologia ATM nelle LAN avviene normalmente a passi, partendo da una situazione di reti locali classiche realizzate con cablaggio strutturato e concentratori, iniziando a sostituire i concentratori con altri dotati di architettura interna ATM e introducendo ATM sulle dorsali.

Questo primo passo ha il vantaggio di far crescere moltissimo la capacità trasmissiva dei concentratori e delle dorsali (da centinaia di Mb/s a qualche Gb/s) facendo sì che ogni sistema collegato veda la rete locale classica cui è collegato come a lui interamente dedicata.

Il passo successivo prevede di dotare i nuovi posti di lavoro direttamente di schede ATM con velocità comprese tra i 25 e i 155 Mb/s e quindi di non installare più concentratori 802.3/ATM, ma solo switch ATM e di integrarli sia tra loro sia con i vecchi concentratori 802.3/ATM con canali ATM su fibra ottica a 155 Mb/s (figura 20.2).

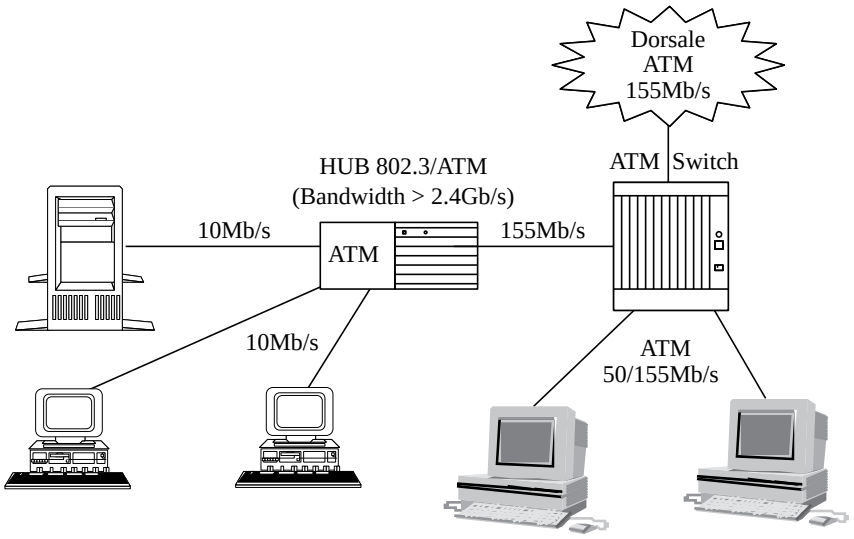


Fig. 20.2 - LAN ibrida ATM e 802.3.

L'ultima fase sarà l'adozione sistematica di ATM con velocità minima di 50/155 Mb/s per i posti di lavoro e con aggiornamento delle dorsali a 622 Mb/s prima e a 2.4 Gb/s poi (figura 20.3).

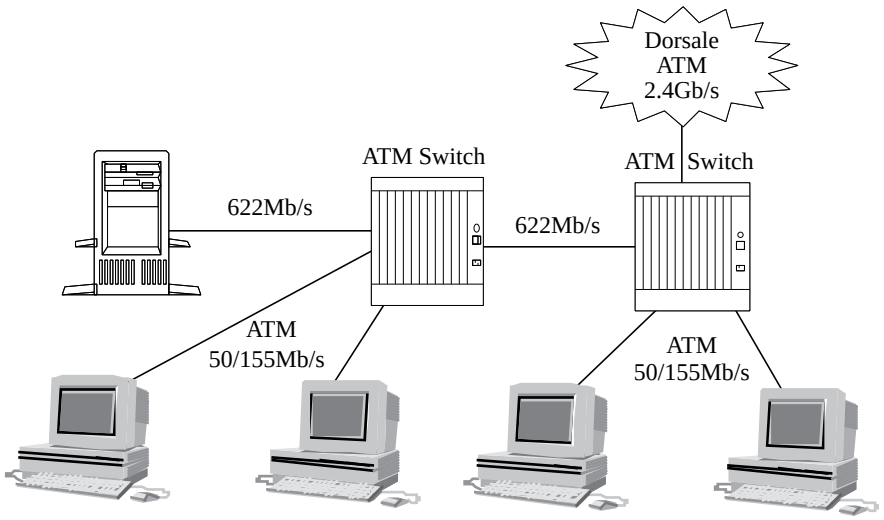


Fig. 20.3 - LAN interamente ATM.

Per poter far convivere le LAN classiche con quelle ATM e per poter far sì che le LAN ATM vengano viste dai protocolli di livello superiore come LAN classiche, l'ATM Forum ha sviluppato uno standard per la "LAN Emulation" [1] che verrà descritto nel resto del capitolo.

20.4 LAN EMULATION SU ATM

La necessità di uno standard per emulare i servizi offerti dalle LAN tradizionali su ATM nasce dalla constatazione che oggi la maggior parte del traffico dati in sede locale è veicolato tramite reti locali conformi agli standard IEEE 802.3 e IEEE 802.5.

20.4.1 Caratteristiche

Nel paragrafo 20.1 abbiamo già visto che le LAN classiche differiscono in vari aspetti dalle LAN ATM: da qui la necessità di definire una *Emulated LAN* (ELAN), cioè un servizio ATM che emula i servizi offerti da una LAN classica. L'emulazione è realizzata da appositi strati software che devono essere associati alle interfacce ATM.

Quando una rete ATM fornisce un servizio di ELAN si hanno vari benefici:

- si può realizzare un sistema misto basato sull'interconnessione di LAN classiche e di reti ATM tramite bridge, il quale garantisce interoperabilità tra tutte le stazioni, indipendentemente dal tipo di connessione usata;
- la migrazione di una stazione da una rete locale classica ad una rete locale ATM può avvenire semplicemente sostituendo la sua scheda di rete, ma senza effettuare alcuna modifica al suo software di rete.

Per raggiungere questo scopo ambizioso una ELAN deve fornire i seguenti servizi:

- *connectionless services*: una stazione collegata ad una ELAN deve poter trasmettere i pacchetti senza aprire a priori una connessione;
- *multicast services*: una stazione collegata ad una ELAN deve poter inviare pacchetti in multicast o in broadcast, tramite indirizzi multicast, broadcast o funzionali (si veda il paragrafo 7.2.6);
- compatibilità con le *MAC driver interface* più diffuse ed in particolare con NDIS, ODI e Packet Driver;

- possibilità di creare domini o LAN virtuali, cioè di definire sulla stessa rete ATM più ELAN, ciascuna associata ad un dominio, all'interno delle quali è confinato il traffico di multicast/broadcast: domini diversi comunicheranno tra loro, ad esempio, tramite router;
- interoperabilità a livello MAC tra stazioni connesse a LAN e stazioni connesse ad ELAN: in particolare una ELAN deve permettere di emulare reti Ethernet/IEEE 802.3 e Token Ring/IEEE 802.5.

20.4.2 Architettura

La realizzazione di detti servizi avviene utilizzando su una scheda ATM l'AAL5 ed appoggiando su di esso una *LAN Emulation Entity*, come schematizzato in figura 20.4

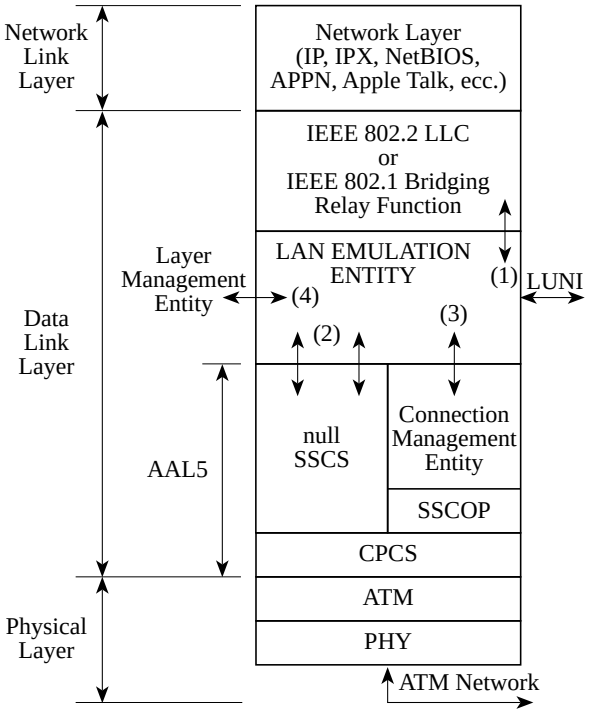


Fig. 20.4 - Architettura LAN emulation.

La LAN Emulation Entity fornisce le primitive che emulano la trasmissione e

la ricezione di pacchetti MAC e su di essa si appoggiano i livelli superiori che possono essere:

- nel caso di stazioni o router, l'IEEE 802.2 che fornisce l'imbustamento multiprotocollo (si veda il capitolo 5);
- nel caso di bridge, le funzioni di "relay" in accordo allo standard IEEE 802.1 (si veda il capitolo 10).

La LAN Emulation Entity utilizza a sua volta i servizi forniti dalla "Layer Management Entity" per le procedure di inizializzazione e controllo e dalla "Connection Management Entity" per il setup e il rilascio delle connessioni virtuali.

Per quanto concerne la trasmissione e la ricezione delle trame MAC, questa avviene utilizzando la cellizzazione offerta da AAL5 tramite il "null SSCS".

20.4.3 Elementi componenti

Una ELAN è composta da un insieme di *LAN Emulation Client (LEC)* e da un singolo *LAN Emulation Service*, come rappresentato in figura 20.5.

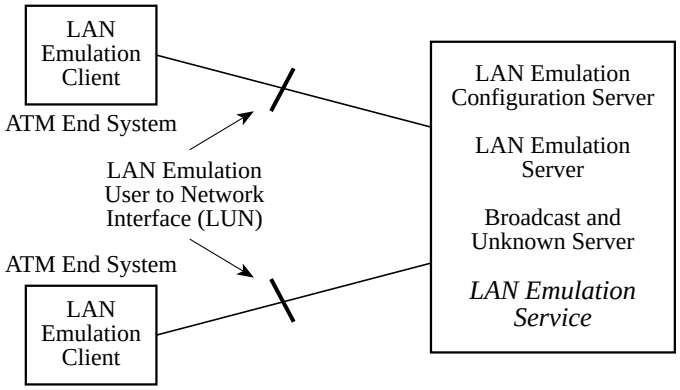


Fig. 20.5 - Componenti LAN emulation.

I LEC devono essere presenti su tutte le stazioni ATM che intendono partecipare ad una ELAN e rappresentano un insieme di utenti. Si possono avere due casi tipici:

- End Station: il LEC è associato ad una stazione di lavoro di un utente

collegata in ATM, quindi rappresenta solo un utente (un unico indirizzo MAC con formato conforme allo standard IEEE 802), e permette la comunicazione tra l'end station ATM ed altre end station collegate sia su LAN convenzionali, sia direttamente sulla rete ATM (purché anche loro dotate della funzionalità di LAN Emulation);

- Intermediate System: il LEC è associato ad una scheda ATM di un bridge o di un router e quindi consente di raggiungere stazioni collegate su una LAN classica (anche detta "Legacy LAN"). Nel caso del router il LEC rappresenta un unico indirizzo MAC, avvenendo l'instradamento a livello 3, mentre nel caso del bridge il LEC è detto proxy client in quanto rappresenta tutte le stazioni non ATM che sono raggiungibili tramite esso (molti indirizzi MAC, tipicamente uno per ciascuna stazione non ATM).

I LEC svolgono funzioni di emulazione dei livelli MAC di IEEE 802.3 e IEEE 802.5, di trasmissione e ricezione di dati, di risoluzione degli indirizzi MAC in indirizzi ATM e altre funzioni di controllo.

Il LAN Emulation Service è fisicamente un dispositivo hardware, noto ai LEC, che esegue i processi software necessari all'emulazione delle LAN. Su ogni rete ATM possono essere presenti più LAN Emulation Service che permettono la realizzazione di più ELAN (cioè più LAN virtuali). Ognuno può essere realizzato in modo centralizzato (su un'unica stazione), distribuito (su più stazioni), oppure integrato (all'interno dei commutatori ATM). Nel caso di realizzazione distribuita l'attuale versione dello standard non specifica i criteri di distribuzione dei vari server. È ragionevole prevedere che un LAN Emulation Service venga inizialmente realizzato su workstation finché lo standard è in via di definizione, e in seguito venga integrato nei commutatori ATM.

La figura 20.6 mostra un esempio di internetworking di LAN classiche e LAN ATM, indicando la posizione dei LEC e del LAN Emulation Service.

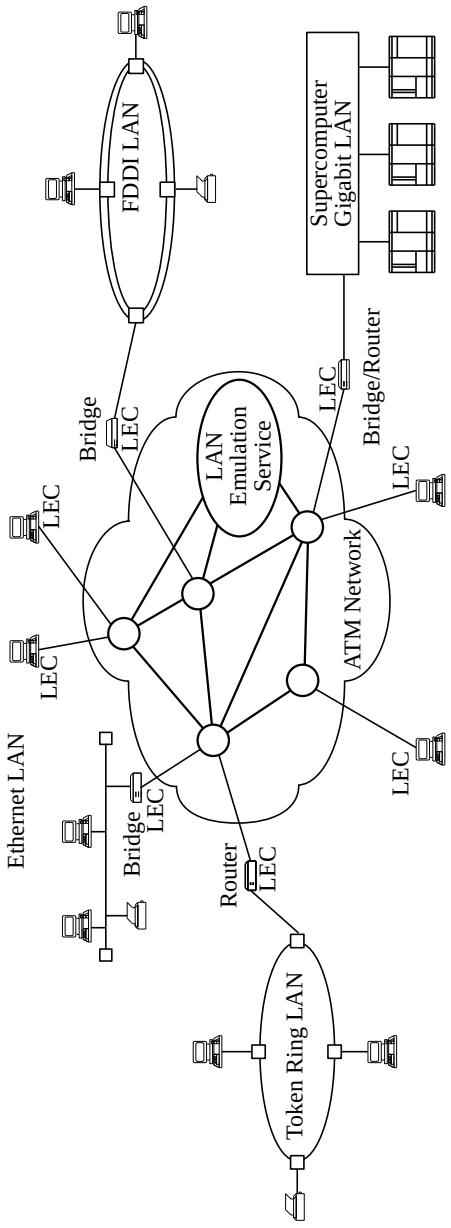


Fig. 20.6 - Internetworking di LAN classiche e LAN ATM.

20.4.4 Interfaccia LUNI

I LEC e il LAN Emulation Service comunicano tramite una interfaccia detta *LUNI (Lan emulation User to Network Interface)* (si vedano le figure 20.4 e 20.5) che definisce i seguenti servizi che vengono messi a disposizione dei LEC dal LAN Emulation Service:

- *Inizializzazione*. Tramite questo servizio ogni LEC individua le ELAN presenti sulla sottorete ATM cui è connesso e può entrare a far parte di una di esse in modo automatico (funzionamento di tipo "plug and play") in modo simile a quanto avviene quando si collega una nuova stazione ad una LAN classica.
- *Registrazione*. Nel momento in cui un LEC entra a far parte di una ELAN, comunica al LAN Emulation Service il proprio indirizzo MAC (nel caso di una stazione), gli indirizzi MAC dei nodi tramite esso raggiungibili (nel caso di un bridge trasparente), oppure dei route descriptor (nel caso di bridge source routing).
- *Risoluzione degli indirizzi*. Il LEC interagisce con il LAN Emulation Service per ottenere l'indirizzo ATM tramite cui raggiungere una stazione che ha un dato indirizzo MAC.
- *Trasferimento dei dati*. I LEC consentono ai protocolli che si appoggiano su LAN Emulation di inviare delle LE-SDU (*Lan Emulation Service Data Unit*) che emulano le MAC-SDU delle reti locali classiche. I LEC mittente e destinatario sono identificati dai rispettivi indirizzi MAC. La LE-SDU viene incapsulata in una AAL5-SDU e trasmessa sulla rete ATM.

20.4.5 Connessioni virtuali

L'interfaccia LUNI utilizza delle VCC (Virtual Channel Connection) di controllo e di dato, per le comunicazioni tra LEC e LEC o tra LEC e LAN Emulation Service. È possibile realizzare una ELAN su una rete ATM che realizzi solo SVC (Switched Virtual Channel), solo PVC (Permanent Virtual Channel) o entrambi.

Il LAN Emulation Service è a sua volta composto dai tre seguenti moduli, che corrispondono a processi software:

- *LES (Lan Emulation Server)*. Entità che realizza funzioni di controllo e coordinamento e fornisce modalità per registrare e risolvere indirizzi ATM, indirizzi MAC e route descriptor;

- *BUS (Broadcast and Unknown Server)*. Entità che gestisce le trasmissioni multicast/broadcast e parte di quelle singlecast (prima che sia stata aperta la VCC diretta tra i LEC);
- *LECS (Lan Emulation Configuration Server)*. Entità di configurazione che assegna i LEC alle ELAN, creando quindi le associazioni tra LEC e LES.

Per ogni ELAN il LAN Emulation Service instanzia una copia di questi tre processi ad essa dedicati.

La figura 20.7 illustra le relazioni esistenti tra LEC, LECS, LES, BUS, LUNI e LAN classiche, evidenziando le VCC che vengono utilizzate per il colloquio tra le varie entità.

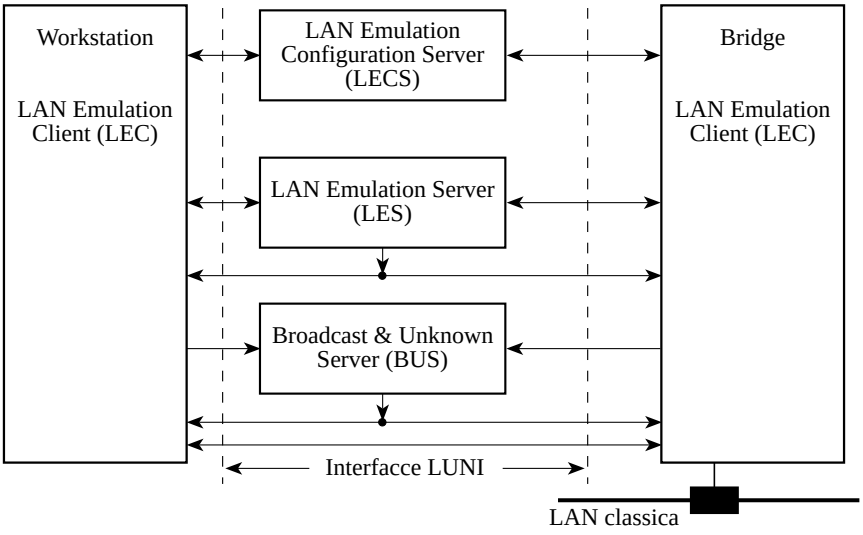


Fig. 20.7 - Connessioni attraverso LUNI.

Ogni LEC ha VCC separate per il traffico dati (emulazione IEEE 802.3 e IEEE 802.5) e per il traffico di controllo (ad esempio, risoluzione di indirizzi). Ogni VCC trasporta il traffico per una singola ELAN.

Le VCC di controllo sono create durante la fase di inizializzazione del LEC e collegano il LEC al LECS e il LEC al LES. Esistono tre VCC di controllo dette: "configuration direct VCC", "control direct VCC" e "control distribute VCC".

La *configuration direct VCC* (figura 20.8) è una VCC bidirezionale tramite la quale il LEC richiede al LECS di entrare a far parte di una ELAN e ottiene da questo l'indirizzo del LES associato alla ELAN prescelta. Il LEC non è obbligato a

mantenere questa VCC dopo la fase di inizializzazione, ma può farlo se intende inviare ulteriori richieste al LECS.

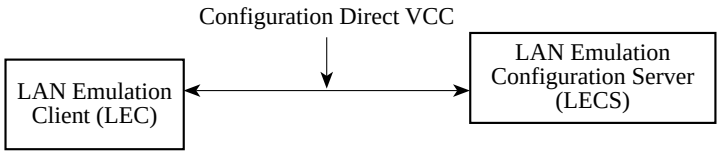


Fig. 20.8 - Configuration direct VCC.

La *control direct VCC* (figura 20.9) è una VCC bidirezionale, creata dal LEC con il LES della ELAN prescelta, per trasmettere traffico di controllo ed in particolare le richieste di LE_ARP (*LAN Emulation Address Resolution Protocol*) utilizzate per trovare le corrispondenze tra indirizzi MAC e indirizzi ATM.

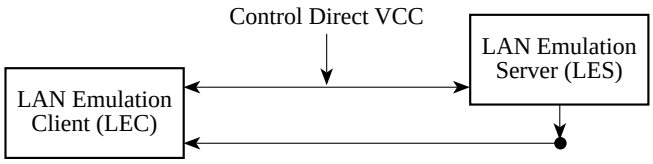


Fig. 20.9 - Control direct VCC.

La *control distribute VCC* (figura 20.10) può essere opzionalmente creata dal LES per trasmettere traffico di controllo verso i LEC e può essere di tipo punto-punto o punto-multipunto.

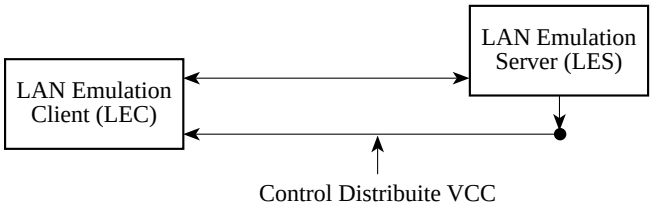


Fig. 20.10 - Control distribute VCC.

Oltre alle VCC di controllo, esistono tre VCC per i dati dette "data connection". Esse sono la "data direct VCC", la "multicast send VCC" e la "multicast forward VCC".

La *data direct VCC* (figura 20.11) è una VCC punto-punto bidirezionale stabilita tra due LEC che si scambiano traffico di tipo singlecast.

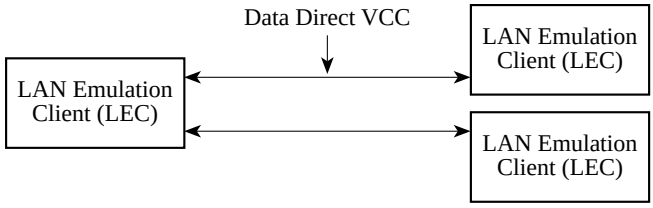


Fig. 20.11 - Data direct VCC.

La *multicast send VCC* (figura 20.12) è una VCC punto-punto monodirezionale dal LEC verso il BUS utilizzata dal LEC per trasmettere il traffico di multicast/ broadcast e il traffico singlecast iniziale (in attesa che venga creata l'opportuna data direct VCC).

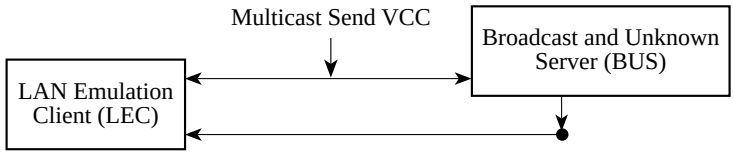


Fig. 20.12 - Multicast send VCC.

La *multicast forward VCC* (figura 20.13) è una VCC punto-punto o punto-multipunto dal BUS verso il LEC utilizzata per trasmettere il traffico di multicast/ broadcast e il traffico singlecast iniziale.

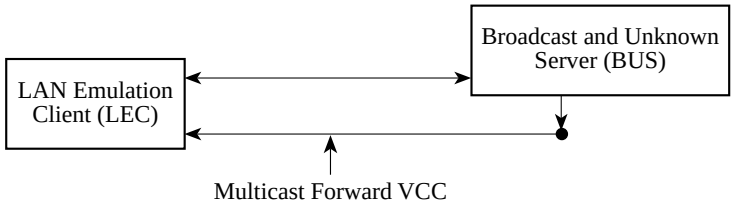


Fig. 20.13 - Multicast forward VCC.

In ambiente SVC il BUS sfrutta la trasmissione punto-multipunto di ATM, in ambiente PVC deve invece gestire direttamente l'invio dei messaggi a tutti i destinatari.

20.4.6 Modalità di funzionamento

Fase di inizializzazione

Quando una stazione ATM viene accesa, o più in generale inizializzata, essa attiva il livello ATM, quindi gli AAL e infine, se richiesto, il software di LAN Emulation ed in particolare la funzionalità di LEC. Il LEC acquisisce dei parametri di configurazione che possono comprendere indirizzi MAC, "emulated LAN name", "max frame size", ecc., e stabilisce un configuration direct VCC con il LECS, utilizzando l'indirizzo ATM del LECS che è definito dallo standard (è cioè un "well known ATM address").

Tramite la configuration direct VCC il LEC ottiene l'elenco delle ELAN presenti sulla rete ATM e può a questo punto chiedere di entrare a far parte di una di esse. Il LECS restituisce l'indirizzo ATM del LES responsabile di tale ELAN. Per ammettere configurazioni di tipo "plug and play" esiste anche la possibilità che sia il LECS a decidere autonomamente in quale ELAN inserire il LEC, in base alla sua collocazione fisica (indirizzo ATM) o alla sua identità (indirizzo MAC).

Fase di registrazione

Il LEC inizia la sua partecipazione ad una ELAN stabilendo una control direct VCC con il LES responsabile di tale ELAN. Tramite tale VCC il LEC registra sul LES uno o più indirizzi MAC ed eventualmente dei route descriptor (nel caso di emulazione IEEE 802.5 con source route bridging). Il LES risponde con l'apertura di una control distribute VCC verso il LEC.

L'ultima operazione che è necessaria per rendere operativo il LEC è l'apertura di una multicast send VCC con il BUS, a cui il BUS risponde con l'apertura di una multicast forward VCC verso il LEC. L'indirizzo ATM del BUS viene determinato dal LEC tramite una chiamata a LE_ARP con l'indirizzo MAC di broadcast (tutti i bit a uno) come parametro.

Fase di trasferimento dati

A questo punto il LEC è pronto a trasmettere delle trame MAC di tipo connectionless. Quando riceve dai livelli superiori la richiesta di trasmissione di una trama MAC, se l'indirizzo MAC di destinazione è di multicast/broadcast, la invia sulla multicast send VCC verso il BUS. Il BUS la ridistribuisce a tutti i nodi della ELAN tramite la multicast forward VCC.

Se la trama MAC ha un indirizzo di tipo singlecast (cioè è destinata ad un'altra stazione), il LEC verifica se ha già aperto una data direct VCC con l'indirizzo MAC

di destinazione e, in caso affermativo, invia la trama sulla data direct VCC. In caso contrario il LEC attiva le procedure per creare la data direct VCC, ma per non ritardare la trama la invia comunque al BUS tramite la multicast send VCC e il BUS la recapita a destinazione tramite la multicast forward VCC. La data direct VCC rimane disponibile per le trame successive, finché non viene automaticamente chiusa se il periodo di inutilizzo supera una soglia predefinita.

Fase di risoluzione degli indirizzi

La creazione di una data direct VCC verso un altro LEC richiede per prima cosa la traduzione dell'indirizzo MAC nel corrispondente indirizzo ATM. Questo avviene con l'aiuto del LES inviando la richiesta di traduzione (LE_ARP) al LES tramite la control direct VCC, a cui il LES risponde tramite la control VCC. Si noti che il LES apprende automaticamente le corrispondenze tra indirizzi MAC e indirizzi ATM in fase di inizializzazione, quando il LEC registra gli indirizzi MAC.

Se il LES non conosce l'indirizzo ATM di un client allora, in conformità allo schema adottato nei transparent bridge IEEE 802.1D, si tenta comunque di far giungere la trama a destinazione inviandola al BUS e da questo a tutti i proxy client (cioè a tutti i bridge).

Se una ELAN emula una LAN IEEE 802.5 allora è prevista anche la presenza di source routing bridge. Il LES, a fronte di una LE_ARP, può ritornare un campo Routing Information formato da un campo control e da una lista di Route Descriptor, uno per ogni bridge source routing da attraversare.

20.4.7 LE-PDU

Le LE-PDU vengono imbustate all'interno delle AAL5-SDU che hanno una dimensione massima fissata a 65535 ottetti. Tuttavia per mantenere la compatibilità con le LAN tradizionali e facilitare l'interoperabilità tramite bridge con esse, le dimensioni massime ammesse per le LE-PDU sono le stesse delle LAN tradizionali. Quindi, nelle connessioni tra LEC e LEC e tra LEC e BUS, le LE PDU devono avere le seguenti dimensioni massime:

- 1536 ottetti (32 celle) per emulazione di LAN IEEE 802.3/Ethernet;
- 4560 ottetti (95 celle) per emulazione di LAN IEEE 802.5/Token Ring a 4 Mb/s;
- 18240 ottetti (380 celle) per emulazione di LAN IEEE 802.5/Token Ring a 16 Mb/s.

Per facilitare l'interoperabilità tra una ELAN su cui sono utilizzati i protocolli TCP/IP ed una sottorete ATM su cui il protocollo IP è usato in modalità nativa, secondo lo RFC 1621 (si veda il capitolo 21), la dimensione massima delle LE-SDU è fissata a 9264 ottetti (193 celle).

BIBLIOGRAFIA

[1] ATM Forum Technical Committee, Lan Emulation Sub-working Group, "LAN emulation over ATM - Version 0", 7/10/94

[2] Biagioni, E. Cooper, R. Sansom: "Designing a Pratical ATM LAN", IEEE Network Magazine, March 1993.

21

INTERNETWORKING CON ATM*

Abbiamo già visto come la tecnica ATM possa essere utilizzata su scala locale, metropolitana e geografica. Per poter sfruttare ATM congiuntamente alle architetture di rete (TCP/IP, SNA, DECnet, IPX, ecc.) occorre però che queste si adattino alla nuova tecnologia. Sono stati seguiti due approcci:

- realizzare uno strato software che, emulando su ATM le funzionalità delle reti locali, consenta di trasportare qualsiasi protocollo di rete (tale approccio, proposto dall'ATM Forum, è stato descritto nel capitolo 20);
- modificare le architetture di rete introducendo il supporto nativo per ATM.

Questo secondo approccio è stato usato, per esempio, da IBM nella sua architettura APPN (si veda il paragrafo 18.5) ed è oggetto di discussione da parte del gruppo di lavoro "IP over ATM" dell'IETF (Internet Engineering Task Force) con particolare riferimento all'architettura di rete TCP/IP. Tale gruppo di lavoro produce periodicamente un documento [1] che riassume lo stato dei lavori in questo settore e che è alla base di questo capitolo.

21.1 TERMINOLOGIA

Questo paragrafo fornisce la definizione di alcuni termini che verranno utilizzati nel seguito:

* Alla stesura di questo capitolo ha fornito un valido contributo l'ing. Davide Bergamasco, che ha svolto la sua tesi di laurea su questo tema presso il Politecnico di Torino. A Davide vanno i più sentiti ringraziamenti degli autori per la preziosa collaborazione.

- rete *broadcast*: rete che può essere composta da un numero arbitrario di stazioni e fornisce la funzionalità di trasmettere con un'unica operazione un pacchetto a tutte le stazioni. Le LAN sono un esempio di reti di questo tipo.
- rete *Non Broadcast Multiple Access* (NBMA): rete simile ad una rete broadcast, ma non fornisce la possibilità di trasmettere un pacchetto a tutte le stazioni. Fanno parte di questa categoria le reti X.25.
- rete *multicast capable*: rete che fornisce delle primitive per trasmettere con un'unica operazione un pacchetto ad un sottoinsieme delle stazioni della rete.

21.2 APPROCCI POSSIBILI

Quando si utilizza la tecnologia ATM, l'internetworking di reti locali e geografiche si arrichisce di interessanti possibilità e di molte complicazioni.

ATM può assumere il doppio ruolo di tecnologia con cui sono realizzate le reti da collegarsi (ad esempio LAN ATM), e di tecnologia con cui viene effettuato l'internetworking su base locale (dorsale di LAN in ATM) o su base geografica (servizio pubblico ATM).

Viste le molte combinazioni possibili, la trattazione che segue non è esaustiva, ma introduce comunque i tre livelli principali a cui può avvenire l'internetworking: livello 2 - sottolivello ATM, livello 2 - sottolivello 802.1D e livello 3.

21.2.1 Internetworking al sottolivello ATM

La prima soluzione è possibile solo se entrambe le reti da collegare sono in tecnologia ATM. Essa consiste nell'utilizzare uno switch che faccia transitare le celle ATM tra le due reti (figura 21.1).

Un vantaggio di questo approccio è la totale trasparenza non solo ai protocolli di livello superiore (IP, OSI, IPX, ecc.), ma anche ai vari AAL e quindi ai vari tipi di applicazione (video, voce e dati). Inoltre, essendo l'internetworking effettuato dall'hardware degli switch, le prestazioni sono molto elevate. Per quanto concerne i limiti, oltre a quello già citato per cui le due reti da interconnettersi devono essere entrambe in tecnologia ATM, occorre evidenziare i potenziali problemi di sicurezza nel caso che una delle reti ATM sia un servizio pubblico che offre la possibilità di stabilire SVC.

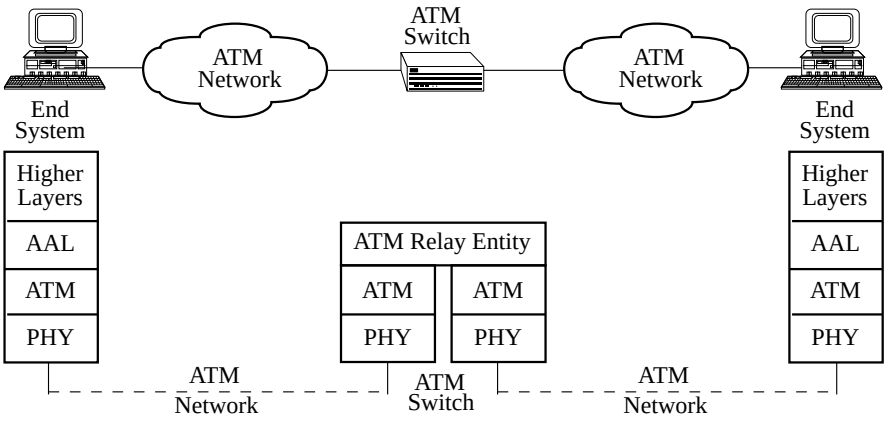


Fig. 21.1 - Internetworking mediante switch ATM.

21.2.2 Internetworking mediante bridge

Per interconnettere una rete locale con una rete ATM, il livello più basso a cui effettuare l'internetworking è quello dei bridge IEEE 802.1D (si veda il capitolo 11). Abbiamo già trattato questa soluzione nel capitolo 20, mostrando come, per colmare le differenze tra le due tecnologie, occorra far ricorso ad un servizio di "LAN Emulation". La figura 21.2 mostra un esempio di internetworking effettuato a tale livello e la stratificazione software corrispondente.

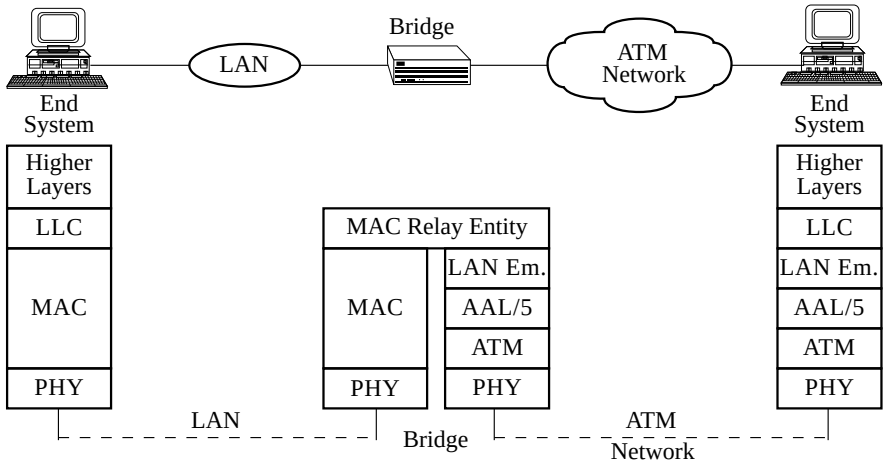


Fig. 21.2 - Internetworking mediante bridge.

Le prestazioni di questa soluzione continuano a rimanere elevate (i bridge elaborano poco - e quindi velocemente - i pacchetti), è ovviamente possibile trasferire solo dati (non voce o video in tempo reale), ma viene mantenuta la trasparenza ai protocolli di livello superiore. Il livello di sicurezza offerto da questa soluzione non è significativamente maggiore di quello della soluzione precedente.

Inoltre questa soluzione, come la precedente, tende a creare delle LAN emulate di grandi dimensioni che spesso non possono essere usate in modo efficace dai protocolli di alto livello. Ad esempio, il protocollo IP ha la necessità di definire una corrispondenza tra le subnet IP e le LAN e spesso le network IP hanno una netmask 255.255.255.0 (si veda il paragrafo 16.5) che impone una dimensione massima della subnet IP, e quindi della LAN, pari a 256 indirizzi.

21.2.3 Internetworking mediante router

L'ultima possibilità è offerta dall'utilizzo dei router e risulta la più idonea quando si debbano affrontare topologie magliate complesse, in cui sono presenti mezzi trasmissivi differenziati. Inoltre, l'utilizzo di router permette di affrontare meglio i problemi della sicurezza, anche se in linea di principio tende a penalizzare le prestazioni. Infatti se si considera la stratificazione dei protocolli in figura 21.3 si vede che, nel caso un router interconnetta due reti ATM, esso deve ricostruire la trama IP partendo dalle celle ATM, determinarne l'instradamento e quindi riframmentare il pacchetto IP in celle ATM. Questo è costoso e non introduce alcun vantaggio se non quello di non modificare i protocolli esistenti.

21.2.4 Osservazioni

Guardando al futuro delle reti e dell'internetworking vedremo una sempre maggior quantità di reti ATM interconnesse tra di loro direttamente a livello ATM, cioè tramite switch. Questa struttura crea la possibilità di poter stabilire circuiti virtuali diretti tra coppie qualsiasi di nodi, i quali attraversano i confini delle subnet IP. In base a quanto discusso nel capitolo 16, questo è da considerarsi una violazione del Modello IP Classico in cui due subnet IP separate possono comunicare solo attraverso un router.

Per risolvere tale problema sono possibili due approcci. Il primo mira ad ammettere la connettività diretta, anche se questa supera i limiti delle subnet IP,

sfruttando le possibilità offerte da certe reti NBMA, tra cui ATM. In pratica, si tratta di estendere l'Address Resolution Protocol (ARP) oltre ai limiti della subnet IP.

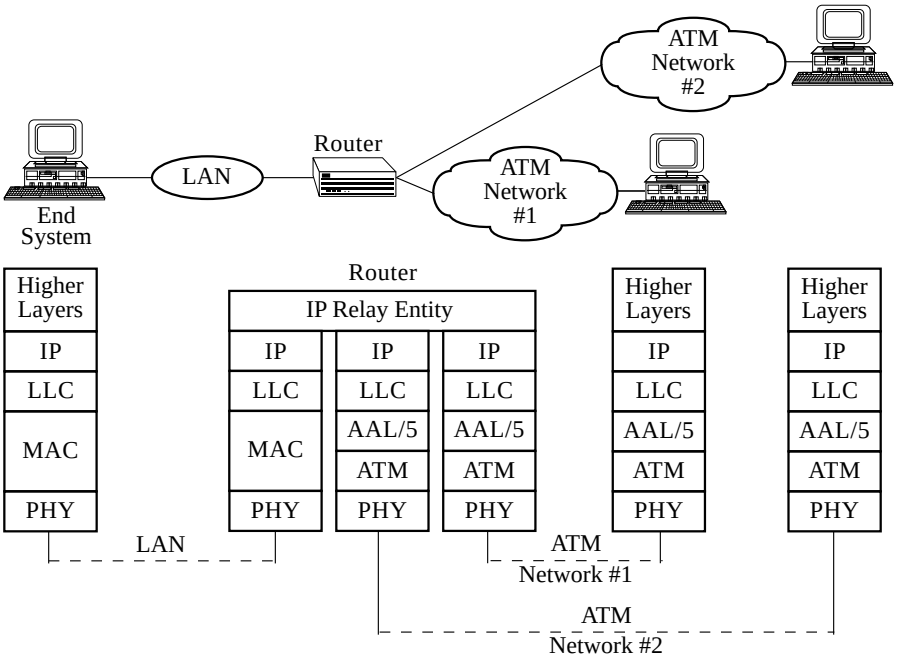


Fig. 21.3 - Internetworking mediante router.

Il secondo si basa su *IP routing* e *IP forwarding*, cioè sull'interconnessione tramite router modificati di subnet IP. Questo secondo approccio deve sempre essere scelto quando:

- le dimensioni dell'internetworking sono significative;
- si utilizzano mezzi trasmissivi differenziati, non essendo possibile utilizzare un'unica tecnologia di rete;
- ragioni di affidabilità non consentono di utilizzare una topologia stellare ed impongono una topologia magliata.

Questi due approcci richiedono comunque la risoluzione di un insieme di problemi comuni che verranno descritti nel prossimo paragrafo. In particolare occorre considerare che le stazioni ATM continueranno probabilmente ad essere multiprotocollo e quindi ad avere la necessità di trametterе e ricevere, oltre ai pacchetti IP, anche quelli di altri protocolli, quali DECnet, IPX, OSI, ecc.

Occorre infine sottolineare che era stata tentata una classificazione degli approcci di IP su ATM differenziandoli per LAN, MAN, WAN. Tale classificazione è stata abbandonata in quanto impropria: la distanza nelle reti ATM incrementa il ritardo di propagazione e diminuisce le prestazioni, ma non cambia sostanzialmente l'organizzazione della rete stessa e le problematiche gestionali o di instradamento del traffico.

21.3 INCAPSULAMENTO ED IDENTIFICAZIONE DEI PROTOCOLLI

L'incapsulamento dei pacchetti e l'identificazione dei punti terminali dei circuiti virtuali sono due problematiche comuni a tutti gli approcci e indipendenti dalle considerazioni di topologia e di routing.

21.3.1 VC multiplexing

Nello standard UNI [9] è previsto che il punto di terminazione di una VC sia stabilito durante la fase di call setup. Un approccio semplice è il *VC multiplexing* o *null encapsulation* che prevede di terminare una VC tramite una istanza di AAL5 direttamente su un protocollo di livello 3 (si veda la figura 21.4). Ad esempio, nel caso dell'architettura TCP/IP, la terminazione della VC è il protocollo IP, si pone cioè direttamente il pacchetto IP all'interno della AAL-SDU.

La realizzazione del VC multiplexing è trattata nello RFC 1483 [2] e nello RFC 1755 [14].

Questo approccio è limitativo in ambienti multiprotocollo dove ogni protocollo richiede la creazione di una VC separata e questo crea un carico di lavoro notevole sugli switch ATM per l'apertura e la chiusura delle VC.

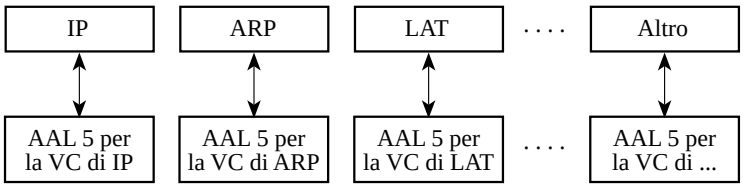


Fig. 21.4 - Reti multiprotocollo mediante VC multiplexing.

21.3.2 Incapsulamento LLC/SNAP

Lo RFC 1483 [2], pur ammettendo il VC multiplexing, propone un approccio alternativo definito *LLC/SNAP encapsulation*. Tale approccio è un adattamento ad ATM di quanto sviluppato nel progetto IEEE 802 e descritto nel paragrafo 5.7.4. Esso consente di trasportare un numero arbitrario di protocolli all'interno di una singola VC, differenziandoli tramite un header LLC/SNAP (la figura 21.5 mostra il trasporto di pacchetti IP su ATM e può essere paragonata con la figura 5.10 che mostra il trasporto di pacchetti IP su LAN IEEE 802).

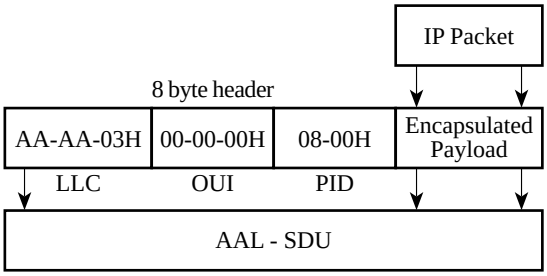


Fig. 21.5 - Incapsulamento LLC/SNAP.

La figura 21.6 mostra un esempio di più protocolli di derivazione Ethernet (OUI = 00-00-00H) che condividono la stessa VC e vengono differenziati in funzione del valore del campo PID (Protocol IDentifier).

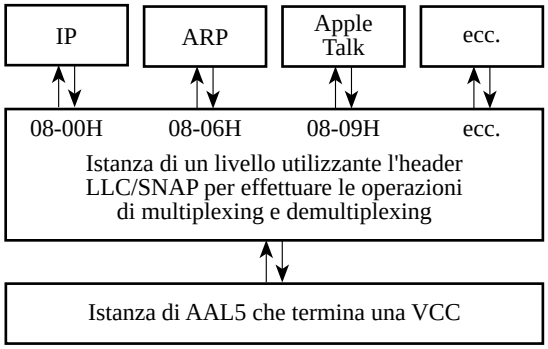


Fig. 21.6 - Condivisione di una VC tramite LLC/SNAP.

21.3.3 Altri metodi di incapsulamento

Il gruppo di lavoro "IP over ATM" ha discusso anche altri metodi di incapsulamento oltre a quelli definiti nello RFC 1483. Tali metodi hanno la caratteristica di eliminare, in larga parte o totalmente, l'overhead dovuto all'header dei pacchetti IP. Infatti, una volta stabilita la VC, gran parte dell'header IP diviene inutile: in particolare gli indirizzi del mittente e del destinatario, non sono più necessari ai fini dell'instradamento del pacchetto.

Sono stati proposti due approcci di incapsulamento che riducono o eliminano l'header IP:

- il primo è denominato TULIP (*TCP and UDP over Lightweight IP*);
- il secondo è noto come TUNIC (*TCP and UDP over Nonexistent IP Connection*).

TULIP

L'approccio TULIP prevede di conservare unicamente il campo indicante il tipo di protocollo di livello 4 trasportato dal pacchetto. Infatti, una volta stabilita una SVC tra due ES, viene a crearsi un collegamento implicito tra le loro entità IP (si veda la figura 21.7) e molti campi dell'header IP possono essere eliminati.

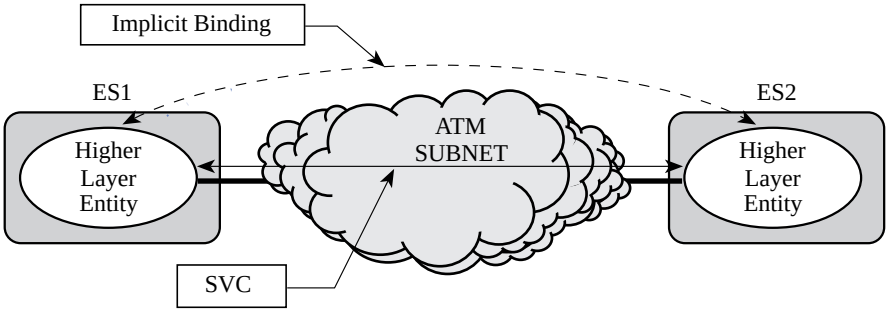


Fig. 21.7 - I modelli TULIP e TUNIC.

Infatti:

- non sussistono ulteriori problemi di instradamento, quindi gli indirizzi IP di mittente e destinatario non servono più;
- la lunghezza di ciascun pacchetto IP è indicata dal campo *lenght* della CPCS-PDU che lo contiene, quindi il campo corrispondente dell'header IP può essere eliminato;

- non avviene la frammentazione in quanto il campo *payload* della CPCS-PDU può contenere un pacchetto IP di dimensione massima (64 K ottetti);
- le condizioni eccezionali possono essere gestite mediante la segnalazione ATM.

TULIP non altera in alcun modo l'architettura di TCP/IP poiché ciascun ES continua a possedere il proprio indirizzo IP e le decisioni sull'instradamento continuano ad essere prese in funzione di tale indirizzo. Viene sfruttata unicamente la caratteristica di ATM di fornire canali di comunicazione end-to-end di tipo punto-punto al fine di eliminare gran parte dell'overhead associato a ciascun pacchetto IP.

TUNIC

L'incapsulamento TUNIC prevede addirittura l'eliminazione dell'intero header IP da ogni pacchetto, assumendo che sussista tra le entità TCP o UDP il collegamento implicito tra due ES, dopo la creazione di una VC. In effetti si tratta di un approccio simile al VC multiplexing spinto ad un livello superiore, ovvero invece di dedicare una VC ad ogni protocollo di livello 3, nel caso di TUNIC viene dedicata una VC a ciascun protocollo di livello 4.

La tabella 21.1 riporta un confronto tra le varie metodologie di incapsulamento*.

Incapsulamento	Informazioni "in banda"	Informazioni "fuori banda"
LLC/SNAP	Indirizzi sorgente e destinazione, famiglia di protocolli di livello 3, protocollo di livello 4, porte di accesso ai servizi	Nulla
VC multiplexing	Indirizzi sorgente e destinazione, protocollo di livello 4, porte di accesso ai servizi	Famiglia di protocolli di livello 3
TULIP	Protocollo di livello 4, porte di accesso ai servizi	Indirizzi sorgente e destinazione, famiglia di protocolli di livello 3
TUNIC	nulla	Indirizzi sorgente e destinazione, famiglia di protocolli di livello 3, protocollo di livello 4, porte di accesso ai servizi

Tab. 21.1 - Metodi di incapsulamento.

* Le espressioni "in banda" e "fuori banda" derivano del gergo in uso presso la telefonia classica e stanno ad indicare due tecniche di segnalazione. La segnalazione in banda è quella effettuata nella stessa banda di frequenze utilizzate per il segnale vocale (es. segnalazione a toni); nella segnalazione fuori banda, l'informazione di segnalazione è veicolata in una banda di frequenze disgiunta da quella destinata al segnale vocale (es. segnalazione ad impulsi in banda base).

21.4 IL MODELLO IP CLASSICO APPLICATO ALLE RETI ATM

L'adattamento del Modello IP Classico alle reti ATM è specificato nello RFC 1577 [12].

Il Modello IP Classico assume che a reti distinte a livello Data Link siano assegnate subnet IP differenti. In particolare si introduce il concetto di *Logical IP Subnetwork* (LIS), ovvero di un insieme di host e router che soddisfano i seguenti requisiti:

- tutti i membri di una LIS (host o router) sono posti sotto il controllo di una singola autorità amministrativa che provvede alla loro gestione e configurazione;
- tutti i membri di una LIS devono condividere la stessa subnet IP e la stessa netmask;
- tutti i membri di una LIS devono essere collegati direttamente alla stessa rete ATM affinché possano comunicare direttamente tra di loro per mezzo di SVC (topologia a maglia completa);
- in ogni LIS deve essere disponibile un meccanismo di risoluzione di indirizzi IP in indirizzi ATM e viceversa affinché sia possibile, all'occorrenza, creare le SVC tra i vari membri;
- tutti gli host di una LIS devono poter accedere ad un router di default che consenta loro di comunicare con destinazioni esterne alla LIS.

Le comunicazioni tra gli host avvengono in base alle seguenti regole (le esemplificazioni fanno riferimento alla figura 21.8):

- host facenti parte della stessa LIS (destinazione "locale") possono comunicare direttamente tra loro attraverso una apposita SVC (es. H1 ed H2);
- un host può comunicare con altri host all'esterno della propria LIS (destinazione "remota") unicamente rivolgendosi al proprio router di default affinché effettui l'instradamento dei pacchetti verso la destinazione finale, anche quando entrambi gli host sono collegati alla stessa rete ATM (es. H2 ed H3 che comunicano attraverso R1*).

Esattamente come nelle subnet IP classiche, la decisione sul fatto che la destinazione sia "locale" o "remota" viene presa sulla base del confronto tra l'indirizzo IP del mittente e della destinazione (si veda il paragrafo 16.5).

---

* Si noti che un router può configurare più interfacce "logiche" connesse a subnet IP diverse su un'unica interfaccia ATM.

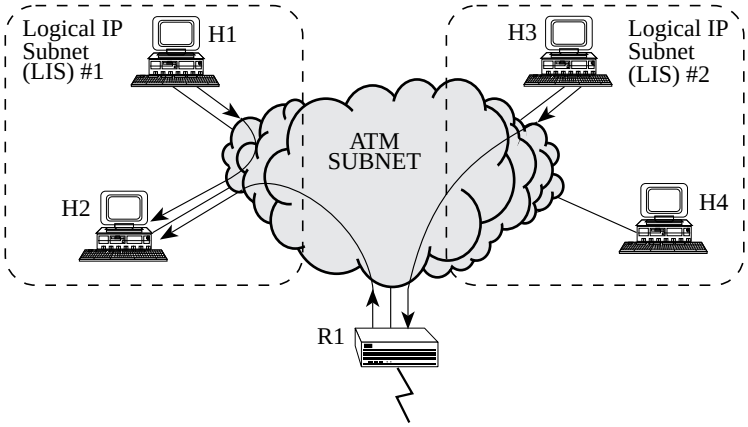


Fig. 21.8 - Modello IP Classico in ambiente ATM.

L'esempio riportato in figura 21.8 è concettualmente analogo a quello di figura 16.6 con la differenza che nel primo tutti gli host ed i router sono collegati alla medesima infrastruttura trasmissiva ATM; nonostante ciò, siccome gli host appartengono a subnet IP (o meglio LIS) differenti, le comunicazioni continuano ad avere luogo esattamente come in figura 16.6, ove le subnet IP sono invece fisicamente distinte.

L'adattamento del Modello IP Classico alle reti ATM dal punto di vista architetturale risulta essere una soluzione semplice in quanto introduce un numero limitato di modifiche, ma dal punto di vista delle prestazioni non sembra essere il più appropriato in quanto, come sarà evidenziato nei seguenti paragrafi, tende a sfruttare il substrato ATM in modo non ottimale.

Il Modello IP Classico, per essere realizzato su reti ATM, necessita di una definizione della Maximum Transmission Unit (MTU) (paragrafo 21.5), di un meccanismo per la risoluzione degli indirizzi IP in indirizzi ATM (paragrafo 21.6) e di opportune procedure di segnalazione (paragrafo 21.7).

21.5 DEFINIZIONE DELLA MTU DI IP SU RETI ATM

Lo RFC 1626 [8] fissa per la *Maximum Transmission Unit* (MTU) del protocollo IP su reti ATM un valore di default pari a 9180 ottetti. Tale valore è stato scelto in base alle seguenti argomentazioni:

- lo RFC 1209 definisce per la MTU di IP su SMDS un valore di default pari a 9180 ottetti; pertanto, ai fini dell'interoperabilità SMDS - ATM è opportuno che i pacchetti IP abbiano le stesse dimensioni;

- la maggior parte dei protocolli e degli applicativi che si appoggiano su TCP/IP, come ad esempio NFS (Network File System), generano PDU di notevoli dimensioni (tipicamente nell'ordine degli 8 KB). Affinché i pacchetti IP in cui esse sono incapsulate non vengano frammentati, è necessario che la MTU di IP su ATM abbia dimensioni non inferiori a quelle di dette PDU;
- i router IP offrono migliori prestazioni se operano su pacchetti di grosse dimensioni dal momento che l'overhead computazionale che essi introducono dipende in misura maggiore dal numero di pacchetti instradati piuttosto che dal numero di byte trasmessi.

Nelle reti ATM, aggiungendo alla dimensione di default della MTU di IP (9180 ottetti) gli otto ottetti dell'header LLC/SNAP si ottiene una dimensione della AAL-SDU (e quindi della CPCS-SDU) pari a 9188 ottetti. Quindi all'atto dell'attivazione di una SVC, se l'ES chiamante desidera utilizzare la dimensione di default della MTU, dovrà specificare nel messaggio di setup il valore 9188.

21.6 RISOLUZIONE DEGLI INDIRIZZI

Lo RFC 1577 [14] stabilisce che la risoluzione degli indirizzi nell'ambito di una LIS realizzata tramite una rete ATM debba essere effettuata mediante i protocolli:

- *ATM Address Resolution Protocol* (ATMARP), per quanto concerne la risoluzione diretta (da indirizzi IP ad indirizzi ATM);
- *Inverse ATM Address Resolution Protocol* (InATMARP), per quanto concerne la risoluzione inversa (da indirizzi ATM ad indirizzi IP).

Tali protocolli, pur essendo funzionalmente identici alle versioni standard ARP ed InARP, dal punto di vista implementativo sono invece differenti poiché:

- ARP ed InARP basano il loro funzionamento sull'utilizzo di trasmissioni broadcast;
- ATMARP ed InATMARP devono necessariamente ricorrere ad un *ATMARP server* (figura 21.9), dal momento che si trovano ad operare in un ambiente caratterizzato da connessioni punto-punto quale quello ATM.

L'ATMARP server è la sede della tabella di corrispondenza tra indirizzi IP ed indirizzi ATM di tutti i membri della LIS (*ATMARP client*) in cui opera; esso, basandosi su detta tabella, ha la responsabilità di rispondere ad ogni richiesta di risoluzione di indirizzo proveniente da un qualunque client della LIS servita. Si noti che in una LIS può operare un solo ATMARP server, mentre quest'ultimo può servire contemporaneamente più LIS.

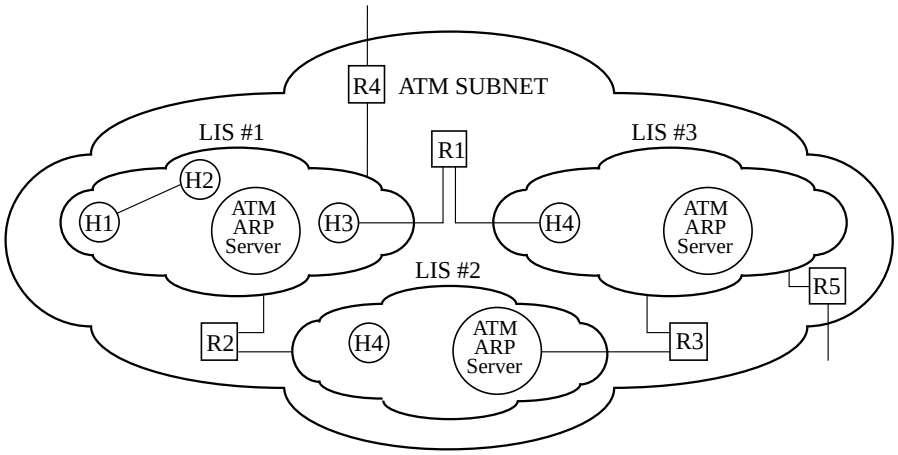


Fig. 21.9 - Modello IP Classico in ambiente ATM.

L'implementazione di ATMARP ed InATMARP si differenzia a seconda del tipo di connessioni virtuali fornite dalla rete ATM.

Se la rete ATM fornisce unicamente connessioni virtuali permanenti, la risoluzione diretta degli indirizzi non è necessaria: esiste una corrispondenza biunivoca ed "immutabile" tra connessioni virtuali e indirizzi IP di destinazione. Ogni stazione crea e mantiene una tabella di corrispondenza tra indirizzi IP e identificatori di connessione virtuale (VCI/VPI) inviando richieste InATMARP su ciascuna delle connessioni virtuali. Dal momento che le entry di tale tabella devono essere sottoposte ad ageing al fine di garantirne un costante aggiornamento, la procedura sopra descritta si ripete periodicamente.

Se invece la rete ATM fornisce connessioni virtuali commutate, le procedure di risoluzione degli indirizzi, sia diretta, sia inversa, sono essenziali ai fini del routing nell'ambito della LIS.

21.6.1 Il server ATMARP

Un ATMARP server costruisce ed aggiorna dinamicamente la tabella di corrispondenza come segue:

- quando un client stabilisce una connessione con il server, il server invia subito al client una richiesta InATMARP (InARP_REQUEST) in modo da determinarne l'indirizzo IP (figura 21.10);

- quando giunge la risposta dal client (InARP_REPLY), il server, che era già a conoscenza dell'indirizzo ATM del client avendolo ricevuto durante la procedura di segnalazione, inserisce oppure aggiorna una entry del tipo <Client_ATM_Address, Client_IP_Address> nella tabella;
- alla entry è inoltre associato l'identificatore della connessione virtuale (VCI/VPI) dalla quale è pervenuta la richiesta, nonché un timestamp da utilizzarsi ai fini dell'ageing della stessa.

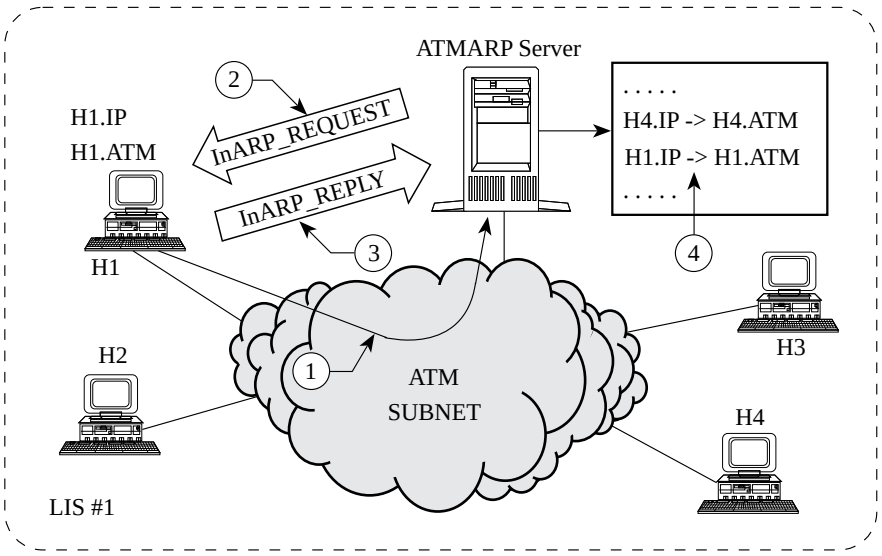


Fig. 21.10 - Registrazione di ATMARP client.

Quando il server ATMARP (figura 21.11) riceve una richiesta di risoluzione di indirizzo diretta (ARP_REQUEST), esso può generare due tipi di risposte:

- ARP_REPLY: è la risposta positiva, contenente l'indirizzo ATM richiesto; essa viene restituita se nella tabella esiste una entry con l'indirizzo IP ricevuto nella richiesta;
- ARP_NAK: è la risposta negativa nel caso contrario.

La risposta negativa, non prevista originariamente da ARP, consente al client di capire se il server è fuori servizio (nessuna risposta ricevuta), oppure se la destinazione non appartiene alla LIS o non ha ancora contattato il server (ARP_NAK).

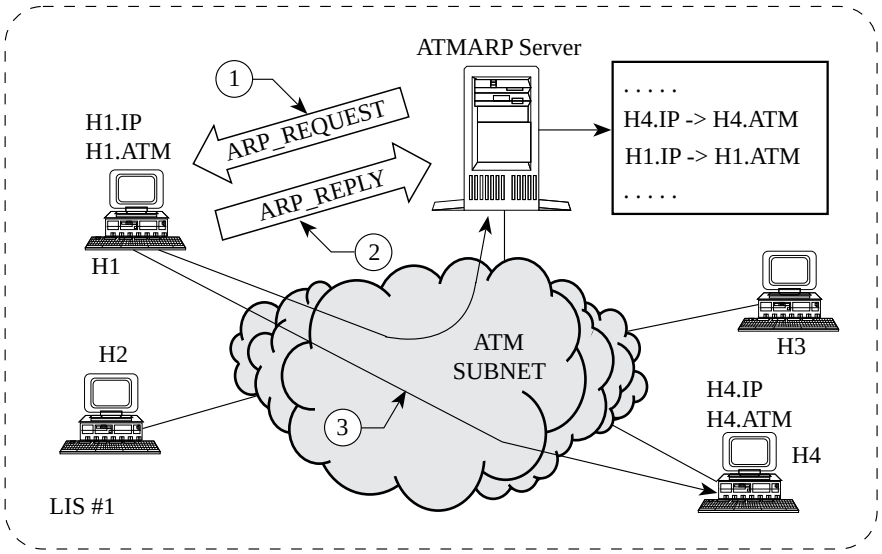


Fig. 21.11 - ATMARP server: risoluzione indirizzo.

21.6.2 Il client ATMARP

Ogni client ATMARP mantiene una tabella locale (cache) contenente le ultime risposte ottenute dal server. Quando il client deve tradurre un indirizzo per prima cosa consulta la tabella locale: se non trova la risposta contatta l'ATMARP server e aggiorna la tabella locale con la risposta ottenuta.

21.6.3 Ageing delle tabelle ATMARP

Sia il server che i client devono tenere costantemente aggiornate le proprie tabelle ATMARP. Le entry della tabella del server sono valide per 20 minuti, mentre quelle delle tabelle dei client lo sono per 15 minuti.

Prima di eliminare una entry scaduta, il server deve generare una richiesta InARP_REQUEST su ogni connessione virtuale associata a tale entry. Se giunge una risposta InARP_REPLY, la entry viene ripristinata, in caso contrario, oppure se non vi sono connessioni associate alla entry, essa viene cancellata.

21.6.4 Trasporto dei pacchetti ATMARP e InATMARP

I pacchetti generati dai protocolli ATMARP e InATMARP devono essere trasportati sulla rete ATM esattamente come i pacchetti IP, ossia mediante il metodo dell'incapsulamento LLC/SNAP (occorre utilizzare come EtherType il valore assegnato ad ARP: 08-06H).

21.7 ASPETTI DI SEGNALAZIONE ATM

In un ambiente caratterizzato da connessioni virtuali commutate due stazioni devono poter stabilire e rilasciare connessioni in funzione del traffico. In ATM questo è possibile grazie al protocollo di segnalazione UNI [9] che dalla versione 3.0 in poi fornisce questa prestazione. Le procedure definite da tale protocollo consentono alla rete di localizzare un destinatario per mezzo del suo indirizzo ATM, di riservare le risorse da destinarsi alla connessione in via di apertura e di svolgere eventualmente negoziazione di parametri tra le stazioni.

Un end system IP connesso ad una rete ATM deve ricorrere alla segnalazione per l'apertura di una connessione virtuale qualora desideri inviare un pacchetto ad un altro end system IP e:

- non esista alcuna connessione stabilita in precedenza;
- esista una connessione aperta, ma questa non possa essere utilizzata (ad esempio perchè caratterizzata da una *Quality of Service* (QoS) non adatta al traffico IP).

Una connessione può invece essere abbattuta mediante segnalazione sia dalla stazione chiamante sia dalla chiamata. È importante che una connessione venga rilasciata dopo l'uso poiché nelle reti pubbliche esiste tipicamente un sistema di tariffazione in base al tempo di utilizzo delle connessioni. Per questo motivo ogni stazione che si interfaccia con reti pubbliche deve incorporare un meccanismo, basato su *inactivity timer*, che provochi la chiusura di quelle connessioni che sono rimaste inattive oltre il periodo di tempo prestabilito. Per le stazioni che operano su reti private il suddetto meccanismo di time-out è opzionale.

L'utilizzo del protocollo UNI da parte del protocollo IP è descritto nello RFC 1755 [14].

21.8 ROUTING E FORWARDING IP SU RETI ATM

Il Modello IP Classico su ATM, di cui si è discusso nel paragrafo 21.4, costituisce una soluzione valida solamente a breve termine in quanto, non comportando significative revisioni architetturali del TCP/IP, risulta essere di facile e rapida attuazione. In un'ottica di lungo periodo, tenendo conto che le esigenze delle applicazioni in termini di banda e di QoS sono in costante crescita, il paradigma di forwarding hop-by-hop* caratteristico del Modello IP Classico risulta invece inadeguato. In particolare tale modello presenta limitazioni intrinseche che sono alla base di un utilizzo inefficiente dell'infrastruttura trasmissiva ATM, tra cui:

- forwarding dei pacchetti IP lungo cammini non ottimali (figura 21.12);
- banda limitata ed elevata latenza a causa dei ritardi introdotti dai router;
- incapacità di sfruttamento di caratteristiche quali banda garantita e QoS tipiche dell'ambiente connection oriented.

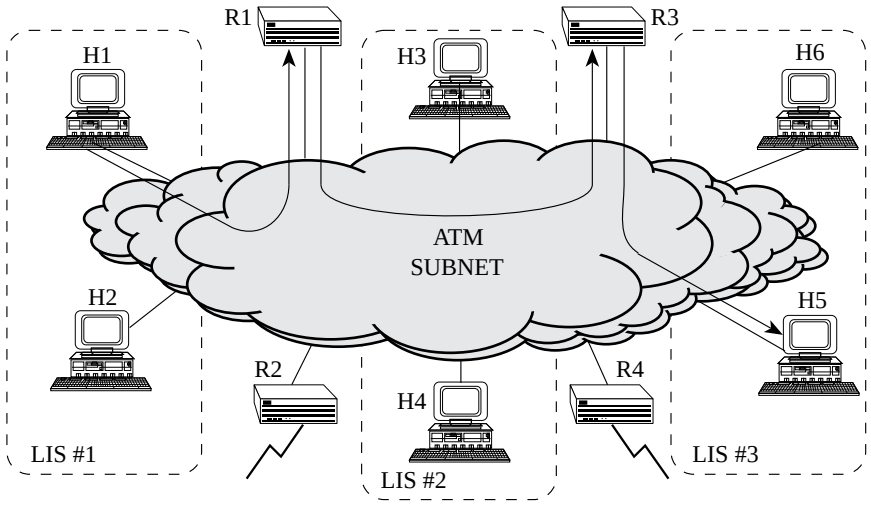


Fig. 21.12 - Esempio di cammino end-to-end non ottimo.

Risulta quindi necessario individuare modelli architetturali caratterizzati da una maggiore flessibilità, capaci di sfruttare appieno le potenzialità intrinseche

* Con il termine hop si indica una tratta trasmissiva tra due stazioni (si veda il paragrafo 14.6); con il termine single-hop un cammino end-to-end composto da una singola tratta trasmissiva; con il termine hop-by-hop un cammino composto da più tratte trasmissive collegate da router.

della tecnologia ATM. L'obiettivo fondamentale di tali modelli deve essere quello di permettere la comunicazione diretta a livello Data Link tra qualunque coppia di sistemi collegati ad una rete ATM, indipendentemente dalla LIS a cui appartengono. L'eliminazione degli hop ridondanti si traduce in un duplice vantaggio:

- miglioramento nelle prestazioni, dal momento che non si hanno più elaborazioni intermedie a livello IP;
- abbattimento dei costi, dovuto all'eliminazione di router non necessari.

Ai fini della sicurezza, tuttavia, la connettività diretta a livello Data Link non è sempre desiderabile: talvolta un hop aggiuntivo è necessario perché il router ad esso corrispondente opera come un firewall (barriera antintrusione).

In generale si possono individuare tre casi di ottimizzazione locale dei cammini. Qualunque siano gli host H e H' ed i *router di frontiera*[*] Rf e Rf' collegati alla stessa rete ATM, deve essere possibile realizzare i seguenti cammini end-to-end con un singolo hop:

- H - H': comunicazione diretta tra host per il trasporto del traffico interno alla rete ATM;
- H - Rf: comunicazione tra host e router di frontiera per il traffico in ingresso/uscita dalla rete ATM;
- Rf - Rf': comunicazione tra router di ingresso e router di uscita per il traffico in transito nella rete ATM.

Una soluzione architetturale in grado di supportare le suddette ottimizzazioni deve inoltre possedere i seguenti requisiti:

- *interoperabilità*: host e router modificati in base alla nuova architettura di routing devono essere compatibili con tutti i dispositivi ancora conformi al Modello IP Classico;
- *praticità*: le modifiche al software di bordo devono essere ridotte al minimo e concentrate soprattutto nei router, dal momento che questi sono in numero notevolmente inferiore e gestiti in modo più centralizzato rispetto agli host;
- *robustezza*: la nuova architettura di routing deve essere robusta nei confronti di errori software, hardware e di comunicazione almeno quanto quella tradizionale;
- *sicurezza*: la nuova architettura deve offrire almeno gli stessi standard di sicurezza presenti in quella tradizionale.

[*] Un router che interconnette tra loro due o più reti IP è detto *router di frontiera*. Nell'esempio di figura 21.7 i router di frontiera sono R2 e R4, mentre i router R1 ed R3 non lo sono in quanto inteconnettono subnet IP nell'ambito della stessa rete IP.

21.9 ALCUNE SOLUZIONI ARCHITETTURALI

Sinora sono state identificate quattro possibili soluzioni architetturali alle problematiche di routing e forwarding IP su reti ATM discusse nel paragrafo precedente:

- *Hop-by-hop redirection*. Tale approccio estende il meccanismo di redirezione classico in modo da far collassare i cammini multi-hop nell'ambito della rete ATM in un cammino single-hop (paragrafo 21.10).
- *Routing esteso*. Si propone di modificare i protocolli di routing per consentire ai router di frontiera collegati ad una rete ATM di scambiarsi i rispettivi indirizzi ATM affinché possano stabilire VC dirette (paragrafo 21.11).
- *Estensioni al protocollo ARP*. Questo approccio mira ad estendere la funzionalità del protocollo ATM ARP all'esterno delle singole LIS, al fine di offrire un servizio che copra l'intera rete ATM. Un esempio di tale approccio è rappresentato dal protocollo NHRP (paragrafo 21.12).
- *Router con capacità di commutazione di cella ATM*. Il quarto ed ultimo approccio propone una modifica all'hardware dei router in modo da consentire a tali dispositivi di "saldare" tra loro i segmenti dei cammini che li attraversano; ciò permette di realizzare cammini end-to-end filtrati a livello IP, ma unificati a livello ATM (paragrafo 21.13).

21.10 HOP-BY-HOP REDIRECTION

L'approccio hop-by-hop redirection tende ad eliminare tutti gli hop non necessari contenuti in un cammino end-to-end tra due sistemi collegati alla stessa rete ATM. Tale schema si basa sulla seguente idea: quando al primo router lungo il cammino giunge un pacchetto dal mittente, esso, dopo aver concluso che l'hop successivo si trova anch'esso all'interno della rete ATM, invia al mittente un messaggio XRedirect (*eXtended Redirect*, una estensione al protocollo ICMP*). Il mittente può a questo punto inviare il pacchetto successivo all'indirizzo specificato

* ICMP (*Internet Control Message Protocol*) è un protocollo che consente a router ed host di scambiarsi informazioni di servizio quali messaggi di errore, controllo e configurazione. Il messaggio redirect è uno dei più importanti in quanto è alla base del meccanismo di *redirezione*. Tale messaggio consente infatti ad un router che riceve un pacchetto destinato ad un host collegato alla stessa subnet dell'host mittente, di segnalare a quest'ultimo che può raggiungere la destinazione desiderata direttamente.

nel messaggio XRedirect; se a tale indirizzo fa capo un altro router il cui attraversamento è inutile, anche questo router invierà al mittente un messaggio XRedirect. L'applicazione iterativa del suddetto procedimento presso tutti i router intermedi si conclude in un cammino single-hop tra mittente e destinazione.

Per realizzare lo schema hop-by-hop redirection occorre modificare il software di bordo dei router e degli host. La modifica principale deve essere apportata al protocollo ICMP affinché supporti il nuovo messaggio XRedirect. Non è possibile utilizzare il messaggio redirect convenzionale in quanto esso può trasportare unicamente gli indirizzi IP associati ai router, mentre lo schema hop-by-hop redirection necessita che i messaggi di redirezione contengano indirizzi IP ed ATM sia dei router sia degli host.

21.11 ROUTING ESTESO

Lo schema hop-by-hop redirection è applicabile solamente quando l'host mittente è membro della rete ATM in quanto è compito suo redirigere via via il proprio traffico, in base ai messaggi XRedirect, verso la destinazione finale. Dal momento che tali messaggi non vengono recepiti dai router, si rende necessario estendere opportunamente i protocolli di routing con un meccanismo analogo. Solo in tal modo è possibile ottimizzare il forwarding del traffico di transito sulla rete ATM tra coppie di router di frontiera.

Facendo riferimento alla figura 21.12, supponiamo, ad esempio, che al router di frontiera R4 giunga dall'interfaccia non collegata alla rete ATM una serie di pacchetti destinati ad una rete facente capo all'altro router di frontiera R2. Supponiamo inoltre che la tabella di instradamento di R4 preveda che per raggiungere R2 esso debba fare riferimento ad R1. Sulla base di tale indicazione R4 invia il primo pacchetto a R1; quest'ultimo nota che il pacchetto è destinato ad R2 e che questi è collegato alla stessa rete ATM di R4. Siccome il cammino R4 - R1 - R2 risulta non ottimale, R1 segnala ad R4, per mezzo di un opportuno messaggio del protocollo di routing esteso, di redirigere il proprio traffico verso R2 e fornisce contemporaneamente l'indirizzo ATM di quest'ultimo. In tal modo R4 può aggiornare la propria tabella di instradamento, cosicché tutti i pacchetti successivi siano inviati direttamente a R2.

21.12 NHRP: NEXT HOP RESOLUTION PROTOCOL

Una rete ATM di grandi dimensioni quale una SVC ATM WAN, è tipicamente ripartita in una pluralità di LIS indipendenti (si pensi ad esempio al caso di varie

ATM LAN, corrispondenti ciascuna ad una LIS, interconnesse mediante una SVC ATM WAN). Il protocollo ATMARP (paragrafo 21.6) consente di risolvere l'indirizzo IP di una destinazione (host o router) nel corrispondente indirizzo ATM solamente se questa appartiene alla LIS del mittente.

Ai fini del superamento della limitazione intrinseca al Modello IP Classico sopra evidenziata, il gruppo di lavoro ROLC (Routing Over Large Cloud) di IETF ha sviluppato il protocollo *NBMA Next Hop Resolution Protocol* (NBMA NHRP), un protocollo di routing e risoluzione degli indirizzi adatto a tutte le tecnologie di networking NBMA che, come ATM, non supportano trasmissioni broadcast [6], [11].

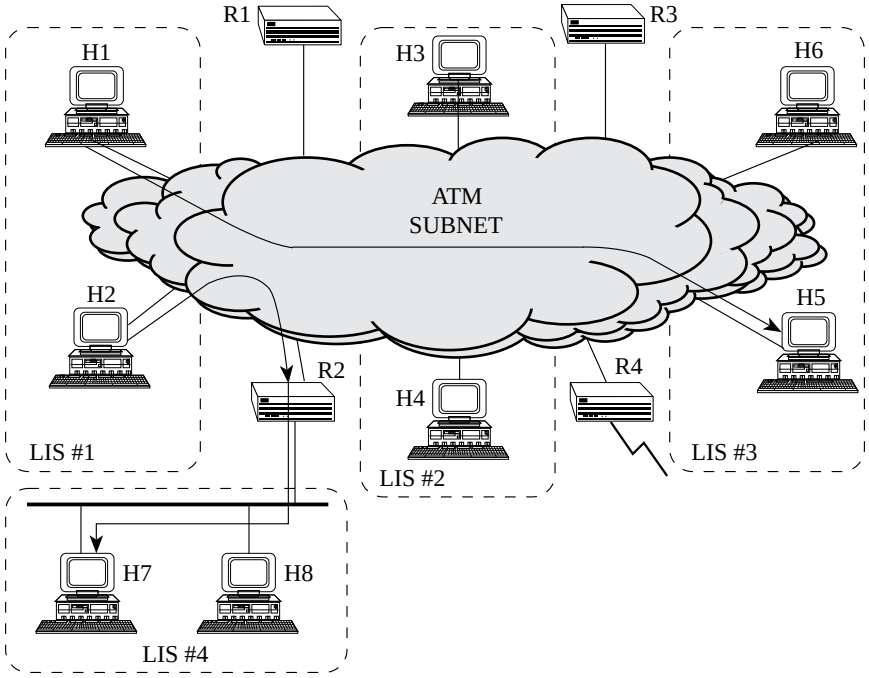


Fig. 21.13 - Esempio di forwarding IP basato sul protocollo NHRP.

NBMA NHRP consente ad una stazione mittente (host o router) che deve comunicare attraverso una rete ATM di determinare gli indirizzi IP ed ATM del cosiddetto *next hop* verso la stazione di destinazione, noto l'indirizzo IP di quest'ultima. Se la destinazione fa parte della rete ATM del mittente, l'indirizzo del next hop restituito da NHRP sarà l'indirizzo ATM della destinazione stessa, altrimenti sarà quello del router di frontiera che si trova sul più breve cammino possibile (in termini di hop) tra mittente e destinazione. Una volta noto l'indirizzo ATM del next hop, la

stazione mittente può attivare una SVC con esso ed avviare la trasmissione di pacchetti IP. Ad esempio, facendo riferimento alla figura 21.13, per mezzo di NHRP, H1 è in grado di apprendere l'indirizzo ATM di H5 e quindi di stabilire una SVC con quest'ultimo invece di inviare i pacchetti lungo il cammino multi-hop H1 - R1 - R3 - H5 come accadeva in figura 21.7. Inoltre H2 viene informato che il "miglior" router di uscita per raggiungere H7 è R2 e non il router di default R1.

Il protocollo NHRP, eliminando dai cammini end-to-end tutti gli hop non necessari, permette di ottimizzare notevolmente il processo di forwarding di pacchetti IP nell'ambito di una rete ATM.

I paragrafi seguenti illustrano più in dettaglio le caratteristiche del protocollo NHRP.

21.12.1 Descrizione del protocollo NBMA NHRP

Il protocollo NBMA NHRP necessita dell'installazione nell'ambito di una rete ATM di una o più entità note come *Next Hop Server* (NHS). Ciascun NHS serve un determinato insieme di host e router (*client*). Gli NHS, oltre a collaborare tra loro per la risoluzione di un next hop nell'ambito della loro rete ATM, possono partecipare a protocolli di routing per apprendere la topologia delle interconnessioni. Infine, gli NHS possono anche affiancarsi agli ARP server, condividendo eventualmente lo stesso hardware, in modo da realizzare una architettura di routing eterogenea in grado di supportare sia host NHRP-capable sia host che operano unicamente in base al Modello IP Classico.

Ciascun NHS gestisce una tabella di corrispondenza tra indirizzi IP ed indirizzi ATM dei client che serve, denominata *next hop resolution cache*, del tutto analoga a quella degli ARP server. Detta tabella può essere configurata manualmente oppure costruita ed aggiornata dinamicamente nei seguenti modi:

- mediante un processo di registrazione attuato dai client mediante l'invio al proprio NHS di un messaggio NHRP_Register;
- estraendo le informazioni dalle richieste di risoluzione ricevute dai client attraverso il messaggio NHRP_Request;
- estraendo le informazioni dalle risposte provenienti dagli altri NHS della rete tramite il messaggio NHRP_Reply.

Si supponga ora che una stazione S debba determinare l'indirizzo ATM del next hop verso D. S si rivolge al proprio NHS inviandogli un messaggio NHRP_Request. Il messaggio NHRP_Request è incapsulato in un pacchetto IP e

trasmesso al NHS attraverso una VC creata all'atto della registrazione, oppure creata ad hoc per la trasmissione della richiesta.

Nel frattempo, in attesa della risposta da parte del NHS, S può procedere come segue:

a) scartare il pacchetto che deve trasmettere a D;

b) trattenere il pacchetto fino a quando non giunge la risposta del NHS;

c) inviare il pacchetto al proprio router di default.

La scelta attuata dipende dalle politiche locali alla LIS cui S appartiene, anche se viene raccomandata la soluzione c) come scelta di default, in quanto consente che il pacchetto giunga comunque a D senza costringere S ad inutili attese. Ovviamente il processo di risoluzione non è attuato per ogni pacchetto trasmesso ad una data destinazione in quanto i client dispongono di una cache locale.

Quando il NHS riceve il messaggio NHRP_Request proveniente da S verifica se nella propria cache è presente una entry contenente l'indirizzo ATM del next hop verso D. Se così non è, il NHS inoltra la stessa richiesta ad un altro NHS. La richiesta passa di NHS in NHS fino a quando non si verifica una delle seguenti condizioni:

- la richiesta giunge al NHS che serve D. Quest'ultimo è in grado di evadere la richiesta generando un messaggio NHRP_Reply contenente gli indirizzi IP ed ATM del next hop verso D. Ovviamente, se D non è collegato alla rete ATM, tale next hop D è l'indirizzo ATM del router di frontiera verso la rete su cui D risiede.
- nessun NHS è in grado di risolvere il next hop verso D. In tal caso l'ultimo NHS visitato genera un messaggio NHRP_Reply di tipo negativo.

In entrambi i casi, il messaggio NHRP_Reply viene inoltrato ad S lungo lo stesso cammino compiuto da NHRP_Request affinché tutti gli NHS attraversati dalla risposta possano inserire nelle loro cache le informazioni in esso contenute. Questo fatto consente agli NHS di rispondere a richieste successive per lo stesso next hop mediante le cosiddette "risposte non autorevoli", ossia risposte che non provengono dal NHS presso cui il client si è registrato. Se un tentativo di comunicazione basato su una risposta non autorevole fallisce (probabilmente perché si sono verificate delle variazioni nella rete), la stazione mittente può inviare una nuova NHRP_Request, richiedendo una risposta autorevole.

In figura 21.14 è rappresentata una situazione esemplificativa di quanto sopra descritto. L'host H1 intende trasmettere un pacchetto all'host H5, ma non ne conosce l'indirizzo ATM. Invia pertanto una NHRP_Request a NHS1 il quale, tuttavia, non dispone di tale informazione. La richiesta viene inoltrata a NHS2 il

quale, essendo il NHS che serve H5, è in grado di generare una NHRP_Reply con l'indirizzo ATM richiesto. Tale risposta, ritornando verso H1, attraversa NHS1 consentendo a quest'ultimo di copiare detto indirizzo nella propria cache per un futuro utilizzo come risposta non autorevole. La risposta giunge infine ad H1, il quale è ora in grado di stabilire una VC con H5 ed inviargli il pacchetto che aveva trattenuto in attesa della risposta.

NHRP consente inoltre di associare l'indirizzo ATM di un next hop ad una intera subnet IP. Ad esempio, se il router X è il next hop tra la stazione S e la stazione D, significa che X è il router di uscita da utilizzare per raggiungere tutte le altre stazioni che condividono lo stesso prefisso di subnet IP di D.

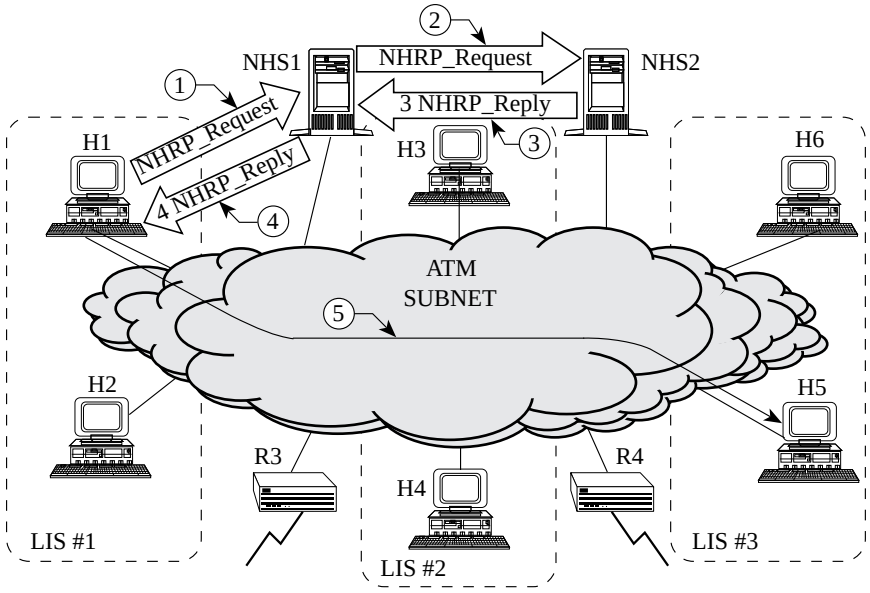


Fig. 21.14 - Esempio di risoluzione dell'indirizzo ATM mediante NHRP.

21.12.2 Modalità di installazione

NHRP prevede due differenti modalità di installazione note come *fabric mode* e *server mode*. Le due modalità si distinguono unicamente nel modo di propagazione dei messaggi NHRP tra gli NHS. È opportuno che i client collegati alla rete ATM non siano a conoscenza del modo in cui NHRP opera, cosicché una variazione nella strategia di installazione possa avvenire in modo del tutto trasparente rispetto agli host.

Server mode

L'installazione di NHRP in server mode presuppone che nell'ambito della rete ATM operi un numero non elevato di NHS e che l'accoppiamento tra NHRP ed il processo di forwarding IP sia molto debole; in particolare in questa modalità non sussiste alcun legame tra i cammini intrapresi dalle richieste attraverso gli NHS ed i cammini seguiti dai pacchetti IP verso destinazioni da questi servite.

Se la rete ATM supporta VC punto-multipunto, ciascun client potrebbe stabilire una VC avente come leaf node tutti gli NHS. In tal modo, una NHRP_Request proveniente da un client solleciterebbe una o più NHRP_Reply dai NHS, in funzione del tipo di risposta che il client si aspetta (autorevole o non autorevole). Tale approccio presenta il vantaggio di ridurre il numero di NHS attraversati da ogni richiesta ad uno solo, ma può risultare oneroso in termini di consumo di risorse della rete qualora i client siano numerosi.

L'inconveniente suddetto può essere eliminato connettendo ogni NHS a tutti gli altri tramite una VC punto-multipunto che l'NHS utilizza per effettuare il forwarding delle richieste che non è in grado di risolvere. Nuovamente, ad ogni NHRP_Request inoltrata sulla VC punto-multipunto possono corrispondere una o più NHRP_Reply in funzione del tipo di risposta che il richiedente si aspetta. Un simile approccio consente di ridurre il numero di NHS attraversati dalle richieste a due solamente e, siccome gli NHS sono pochi, non introduce sulla rete un eccessivo overhead dovuto alla gestione delle VC punto-multipunto.

Fabric mode

L'installazione di NHRP in fabric mode prevede che gli NHS siano localizzati in tutti i router che collegano la rete ATM con il mondo esterno. Questo fatto implica che vi sia un forte accoppiamento tra NHRP ed il processo di forwarding IP, in particolare i cammini intrapresi dai messaggi NHRP_Request verso gli NHS coincidono con i cammini dei pacchetti IP instradati secondo il Modello IP Classico.

Le richieste vengono esaminate da vari NHS/router attraversati sino a quando si verifica una delle seguenti situazioni:

- la NHRP_Request giunge al NHS/router che serve la destinazione indicata: il NHS/router genera una NHRP_Reply positiva;
- la NHRP_Request giunge ad un NHS/router che non è in grado di inoltrarla ulteriormente poiché non conosce alcun cammino di instradamento verso la destinazione finale: il NHS/router genera una NHRP_Reply negativa;

- la NHRP_Request giunge ad un NHS/router che non è in grado di inoltrarla verso il NHS che serve la destinazione a causa dell'assenza di connettività con quest'ultimo: anche in questo caso il NHS/router genera una NHRP_Reply negativa;

In ogni caso la NHRP_Reply viene trasmessa al richiedente esattamente come è stato descritto per il server mode.

21.12.3 Configurazione di NHRP

Alla luce di quanto discusso nei paragrafi precedenti, emergono i seguenti requisiti di configurazione per NHRP:

- ciascun client, indipendentemente dal fatto che si tratti di un host o un router, deve essere configurato con gli indirizzi IP ed ATM di almeno un NHS;
- ogni NHS deve essere configurato con la propria identità e l'insieme di subnet IP servite;
- se NHRP opera in server mode, ciascun NHS deve essere anche configurato con gli indirizzi ATM ed IP di tutti gli altri NHS operanti all'interno della rete ATM;
- se NHRP opera in fabric mode, ciascun NHS che funge anche da router di frontiera per la rete ATM deve essere configurato in modo da poter partecipare ai protocolli di routing intra- ed inter-domain;
- gli NHS possono essere configurati con gli indirizzi ATM dei client da loro serviti sia staticamente (server mode), sia dinamicamente osservando i messaggi NHRP_Request (fabric mode); un'ulteriore modalità di configurazione è basata sulla registrazione esplicita dei client attraverso i messaggi NHRP_Register.

I client NHRP

I client devono ovviamente inserire nelle cache tutte le risposte che ricevono dai server. Devono essere inserite anche entry incomplete, ossia quelle corrispondenti a richieste non ancora evase. Ciò è necessario poiché le stazioni non devono effettuare ulteriori richieste per una data destinazione qualora ve ne sia già una pendente. Inoltre, le stazioni sono tenute a eliminare sia le entry per le quali è scaduto l'holding time, sia quelle indicate nei messaggi NHRP_Purge ricevuti dagli NHS.

Gli NHS finali

Gli NHS che servono una destinazione devono inserire una entry nella propria

cache per tutte le risposte che hanno evaso con informazioni che potrebbero variare nel tempo. Ciò consente agli NHS di inviare un messaggio NHRP_Purge alle stazioni nel momento in cui le suddette informazioni variano. Inoltre, gli NHS sono tenuti ad inserire una entry nella propria cache relativamente a ciascuna stazione dalla quale hanno ricevuto richieste di risoluzione. Tale entry deve essere eliminata allo scadere dell'holding time ad essa associato.

Gli NHS di transito

Un NHS può inserire nella propria cache le informazioni relative alle richieste che instrada verso altri NHS e alle relative risposte. Gli NHS di transito possono rispondere direttamente a richieste non autorevoli, con informazioni tratte dalle proprie cache. Infine essi, come tutti gli altri sistemi NHRP, devono rimuovere tutte le entry per cui sia scaduto l'Holding Time.

Dinamica delle cache

Lo scopo fondamentale di NHRP è quello di risolvere gli indirizzi IP delle stazioni direttamente connesse ad una rete ATM nei corrispondenti indirizzi ATM. Essendo tali associazioni tipicamente piuttosto statiche, una appropriata scelta degli holding time delle entry nelle varie cache tende a minimizzare sia il traffico di richieste e risposte, sia i problemi derivanti dalle variazioni di indirizzo.

Tuttavia, nel caso in cui una destinazione non sia collegata direttamente alla rete ATM, l'associazione tra l'indirizzo IP di quest'ultima e l'indirizzo ATM di un router di uscita verso la rete cui essa appartiene può anche essere molto più dinamica. Ciò provoca un aumento della probabilità che l'informazione presente in qualche cache sia inattendibile. In questo caso, però, la conseguenza di una entry non più valida non è la perdita di connettività con la destinazione, ma semplicemente un cammino di instradamento non ottimale.

È pertanto necessario che un router/NHS, accortosi di una variazione nel percorso di instradamento verso una certa destinazione, invii un messaggio NHRP_Purge al mittente affinché elimini dalla propria cache la entry obsoleta ed effettui una richiesta autorevole per trovare un nuovo router di uscita.

21.13 CELL SWITCHING ROUTER

Un *Cell Switching Router* (CSR) è un apparato di internetworking che integra al suo interno le funzionalità di routing e forwarding IP e di commutatore di celle

ATM [5]. Grazie a dette capacità, un CSR è in grado, in funzione delle informazioni di routing IP, di concatenare una VC in ingresso con una VC in uscita, fornendo quindi connettività a livello ATM anche tra coppie di host che appartengono a LIS differenti, senza violare il Modello IP Classico.

21.13.1 Motivazioni

Le soluzioni architetturali illustrate nei paragrafi precedenti mirano ad eliminare dai cammini end-to-end tutti i router non indispensabili. Non è detto che tale scelta sia sempre la migliore; ad esempio, le funzionalità di forwarding IP tra LIS distinte continuano ad essere richieste nei seguenti casi:

- quando una stazione H1 intende comunque trasmettere pacchetti IP ad una destinazione H2 mentre è in corso la segnalazione per creare una VC diretta H1 - H2; ad esempio, H1 ha inviato una richiesta di risoluzione NHRP dell'indirizzo IP di H2 e, in attesa della risposta, inizia a spedire i pacchetti a H2 tramite un cammino multi-hop;
- quando le esigenze di banda e QoS di talune applicazioni non giustificano lo sforzo di creare una VC tra mittente e destinazione (paragrafo 21.14);
- quando la connettività diretta a livello ATM non è consentita esplicitamente da politiche inerenti la sicurezza.

Inoltre occorre tenere in seria considerazione l'interoperabilità con le tecniche di "*resource reservation*" (RSVP* e STII**) ed il concetto di "*flusso IP*" (IPv6***). RSVP, STII e IPv6 mirano a fornire a livello IP banda e QoS garantite, in modo indipendente dalle reti fisiche sottostanti.

L'introduzione dei CSR è una soluzione diametralmente opposta a quelle viste in precedenza e consiste nell'adeguare il substrato trasmissivo ATM alle preroga-

---

* RSVP (*Resource reSerVation Protocol*) è un protocollo che consente ad un host destinatario di "prenotare" l'utilizzo di risorse, in termini di banda dedicata priorità di servizio, presso i router attraversati dal traffico di pacchetti IP proveniente da un certo mittente.

** STII (*STream protocol version II*) può essere considerato come una versione connection oriented di IP che necessita di una fase di creazione di una connessione tra un mittente ed una destinazione prima della trasmissione dei pacchetti. I router STII-compatibili dislocati lungo il cammino di tale connessione riservano quindi una quota delle loro risorse in accordo alle indicazioni fornite dal mittente.

*** IPv6 (*Internet Protocol version 6*), noto anche come IPng (*IP next generation*), è una evoluzione di IP che prevede nell'header un campo denominato *FlowID*. Come lascia intuire il nome stesso, tale campo indica la presenza di un flusso attivo di pacchetti e viene utilizzato dai router IPv6-compatibili per allocare le proprie risorse in funzione delle caratteristiche di detto flusso.

tive del Modello IP Classico. I CSR si fanno carico di fornire canali di comunicazione end-to-end a livello ATM anche tra host che non condividono la stessa subnet IP. Tale soluzione presenta i seguenti vantaggi:

- miglioramento delle prestazioni nel forwarding dei pacchetti IP in ambienti multi-LIS dovuto all'eliminazione della latenza introdotta dalle elaborazioni a livello IP presso i router;
- possibilità di fornire livelli di banda e QoS adeguati alle applicazioni odierne;
- supporto delle tecniche di resource reservation (RSVP e STII) e dei flussi IP (IPv6);
- conformità all'architettura originaria di TCP/IP che prevede un modello di internetworking imperniato sui router.

21.13.2 Architettura di internetworking basata su CSR

Dal punto di vista architetturale un CSR è simile ad uno switch ATM in quanto è in grado di commutare un flusso di celle proveniente da una VC di ingresso, a cui corrisponde un host mittente, in un flusso di celle su una VC di uscita, associata ad un host di destinazione. A differenza degli switch ATM, nei CSR la concatenazione dei flussi è sotto il controllo dell'entità che effettua il forwarding IP, ossia essa ha luogo solo qualora esista un flusso attivo di pacchetti IP tra mittente e destinazione. Se tale concatenazione avviene presso tutti i CSR attraversati da un cammino end-to-end che unisce mittente e destinazione, si realizza una cosiddetta *ATM bypass-pipe*, ovvero una successione di VC che connettono tra loro CSR adiacenti (nonché mittente e destinazione con i CSR più "vicini"). Il termine ATM bypass-pipe è stato coniato appositamente per distinguere il concetto ad esso sotteso da quello rappresentato dalla convenzionale VC ATM.

In figura 21.15 è mostrata una configurazione di networking basata su CSR. È possibile notare un cammino end-to-end tra gli host H1 e H5 che attraversa le LIS #1, #2 e #3, passando per due CSR. Tale cammino può essere supportato sia tramite una ATM bypass-pipe, sia mediante il convenzionale forwarding hop-by-hop, a seconda delle esigenze delle applicazioni. Infatti tra ciascuna coppia di nodi sono attive due classi di VC:

- *Default-VC*: sono VC utilizzate e condivise tra tutte le applicazioni per le quali il convenzionale forwarding IP hop-by-hop risulta adeguato. Tutti i pacchetti che giungono ai CSR attraverso tali VC sono elaborati a livello IP esattamente come avviene nel Modello IP Classico.

- *Dedicated-VC*: sono particolari VC che vengono concatenate tra loro presso i CSR al fine di costruire una ATM bypass-pipe dedicata ad una particolare applicazione.

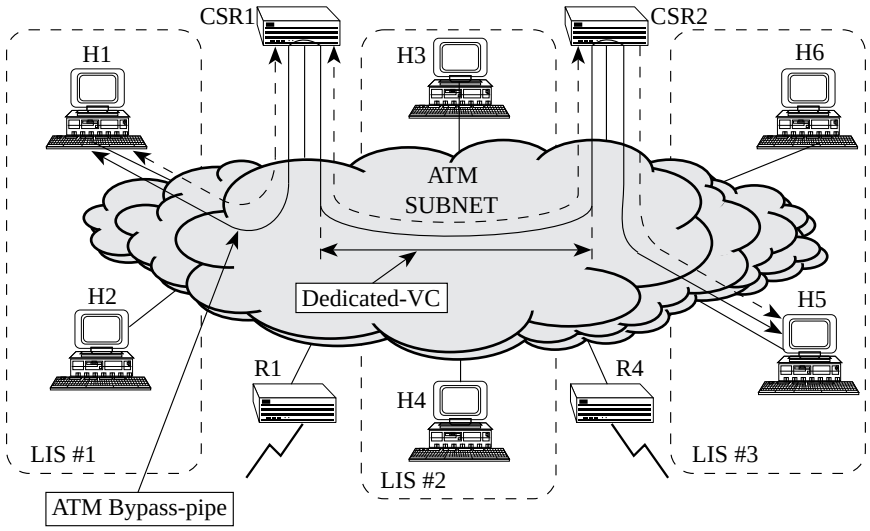


Fig. 21.15 - Esempio di internetworking basato su CSR.

Il cammino seguito da una ATM bypass-pipe dipende dalle tabelle di instradamento dei CSR, e quindi i pacchetti compiono lo stesso percorso dei pacchetti instradati hop-by-hop. Nel caso di figura 21.15, i pacchetti trasmessi dall'host H1 e destinati all'host H2 sono trasferiti lungo il cammino H1 - CSR1 - CSR2 - H2 indipendentemente dal fatto che la comunicazione avvenga hop-by-hop o attraverso una ATM bypass-pipe.

Gestione delle dedicated-VC

Vi sono tre possibili alternative per quanto concerne la gestione delle dedicated-VC:

a) *Creazione di una SVC on-demand.* Ogni volta che deve essere stabilita una ATM bypass-pipe, le dedicated-VC che la compongono vengono create sul momento mediante la normale procedura di segnalazione ATM. Quando la ATM bypass-pipe non serve più, le corrispondenti dedicated-VC vengono rilasciate.

b) *Uso di PVC*. Tra ogni coppia di CSR e tra questi ultimi e gli host, l'amministratore della rete preconfigura un certo numero di PVC. Quando occorre creare una ATM bypass-pipe, le dedicated-VC che costituiscono quest'ultima vengono scelte tra le PVC che in quel momento sono inutilizzate.

c) *Uso di VCI liberi nell'ambito di PVP/SVP*. Tra ogni coppia di CSR e tra questi ultimi e gli host, vengono stabiliti un certo numero di PVP (*Permanent Virtual Path*) o SVP (*Switched Virtual Path*). I PVP possono essere configurati dall'amministratore della rete, mentre gli SVP vengono creati la prima volta che una VC (dedicated-VC o default-VC) deve essere creata tra due nodi. Quando occorre creare una ATM bypass-pipe, le dedicated-VC vengono create all'interno del PVP/SVP.

La scelta del metodo di gestione delle dedicated-VC dipende dal tipo di ottimizzazione che si desidera ottenere.

Nel caso a) viene ottimizzato l'uso delle risorse di rete in quanto le dedicated-VC sono create solo quando servono effettivamente. Tuttavia si ha una elevata latenza nella costruzione della ATM bypass-pipe in quanto per ciascuna delle sue componenti occorre prima effettuare una risoluzione di indirizzo mediante ATM ARP e poi avviare la procedura di segnalazione.

Nei casi b) e c) la latenza è notevolmente inferiore rispetto al caso a) in quanto viene saltata la fase di creazione delle singole dedicated-VC. Tuttavia si manifesta uno spreco di risorse in quanto una quota di banda è staticamente allocata alle PVC o ai PVP, anche se attraverso questi ultimi non transita traffico. Il caso c) risulta comunque preferibile rispetto al caso b) in quanto le risorse di rete e le funzionalità di controllo sono allocate all'intero gruppo di VC rappresentato dalla PVP piuttosto che alla singola PVC.

Creazione e rilascio di ATM bypass-pipe

Le ATM bypass-pipe possono essere create in base al verificarsi di due eventi:

1) esplicita richiesta del livello IP o dei livelli superiori di un host;

2) decisione autonoma di un CSR presa in base a misurazioni condotte sul traffico IP che lo attraversa.

Il caso 1) può essere ulteriormente classificato in base al fatto che il richiedente sia o meno in grado di supportare direttamente una ATM bypass-pipe. Facendo riferimento alla figura 21.16, gli host H2 ed H3 forniscono detto supporto in quanto sono direttamente collegati alla rete ATM. Invece gli host H1 ed H4, pur non facendo parte di quest'ultima, potrebbero comunque trarre vantaggio dalla ATM bypass-pipe R1 - CSR1 - R3; è quindi opportuno che anche ad essi sia consentito partecipare, sebbene per via indiretta, al protocollo di controllo delle ATM bypass-pipe.

Nel primo caso (H2 - H3), l'host mittente ospita un'apposita entità di gestione delle ATM bypass-pipe alla quale il livello IP o i livelli superiori inviano le

richieste. Tale entità comunica con le corrispondenti entità a bordo dei CSR e dell'host di destinazione al fine di stabilire una ATM bypass-pipe tra i due host coinvolti dalla comunicazione.

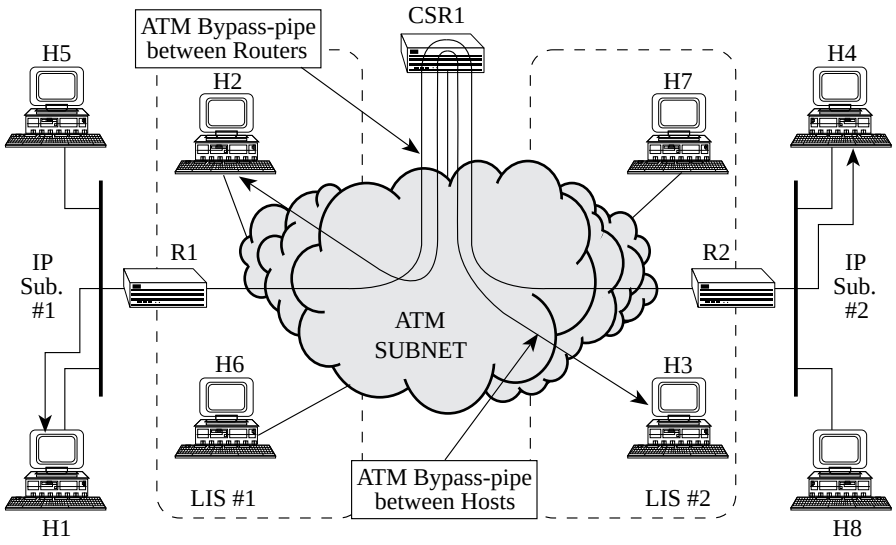


Fig. 21.16 - Esempio di internetworking con CSR e Router convenzionali.

Nel secondo caso (H1 e H4), né il mittente né la destinazione dispongono della suddetta entità. Il livello IP o i livelli superiori possono tuttavia effettuare una richiesta di prenotazione delle risorse tramite STII o RSVP. Tale richiesta si propaga lungo il cammino verso la destinazione (STII) oppure verso il mittente (RSVP) e quando raggiunge il CSR questi la traduce in una corrispondente richiesta di creazione di una ATM bypass-pipe. Il risultato finale è che una richiesta di prenotazione di risorse, effettuata da un host che non partecipa direttamente alla gestione delle ATM bypass-pipe, avvia un processo che si conclude con la creazione di una ATM bypass-pipe tra i CSR della rete ATM attraversati dal traffico.

Per quanto concerne il caso 2), un CSR può iniziare la procedura di creazione di una ATM bypass-pipe sulla base di misurazioni da esso effettuate sul traffico diretto verso una certa destinazione. Ad esempio, facendo sempre riferimento alla figura 21.16, quando CSR1 si accorge che esiste un elevato volume di traffico proveniente dalla subnet IP #1 e diretto verso l'host H3, può richiedere la creazione della ATM bypass-pipe R1 - CSR1 - H3.

Il rilascio delle ATM bypass-pipe è provocato da eventi analoghi a quelli visti sopra. Nel caso 1) il rilascio è causato da esplicite richieste da parte degli host, sia tramite il protocollo di controllo sia attraverso i meccanismi di prenotazione delle risorse. Nel caso 2), invece, un CSR richiede la chiusura di una ATM bypass-pipe qualora noti che il volume di traffico per la quale essa era stata creata scenda al di sotto di un determinato livello.

Da quanto sopra emerge che le richieste per la creazione di una ATM bypass-pipe possono provenire sia dal mittente (ad esempio nel caso STII), sia dalla destinazione (ad esempio nel caso RSVP). Il protocollo deve pertanto supportare entrambi i tipi di richieste.

Richieste provenienti dal mittente

Un mittente, per richiedere la creazione di una ATM bypass-pipe, deve utilizzare il messaggio BP_Setup mediante il quale specifica:

- l'indirizzo IP della destinazione finale;
- l'identificatore della ATM bypass-pipe in fase di creazione;
- l'identificatore della dedicated-VC che intende utilizzare come componente della ATM bypass-pipe;
- la quantità di banda da allocare alla ATM bypass-pipe.

Tale messaggio deve essere trasmesso al primo CSR che si trova sul cammino verso la destinazione finale (figura 21.17). Quando un CSR riceve il messaggio BP_Setup dal nodo che lo precede, determina il next-hop in base alla propria tabella di instradamento e, qualora la banda richiesta sia disponibile, sceglie o crea una dedicated-VC verso il next-hop da usare come componente della costruenda ATM bypass-pipe. Infine invia un analogo messaggio BP_Setup al prossimo nodo. Questa procedura è ripetuta fino a quando il messaggio BP_Setup giunge alla destinazione finale oppure fino a quando un CSR intermedio non constata che la ATM bypass-pipe non può essere estesa ulteriormente, ad esempio a causa di scarsità di banda.

L'ultimo nodo raggiunto dal messaggio BP_Setup risponde con un messaggio BP_SetupAck, il quale compie a ritroso il cammino verso il mittente. Quando tale messaggio giunge al mittente la procedura per la creazione della ATM bypass-pipe può considerarsi conclusa. In figura 21.17 è mostrato un esempio di creazione di ATM bypass-pipe tra i router R1, R2 e CSR1 secondo la procedura sopra descritta.

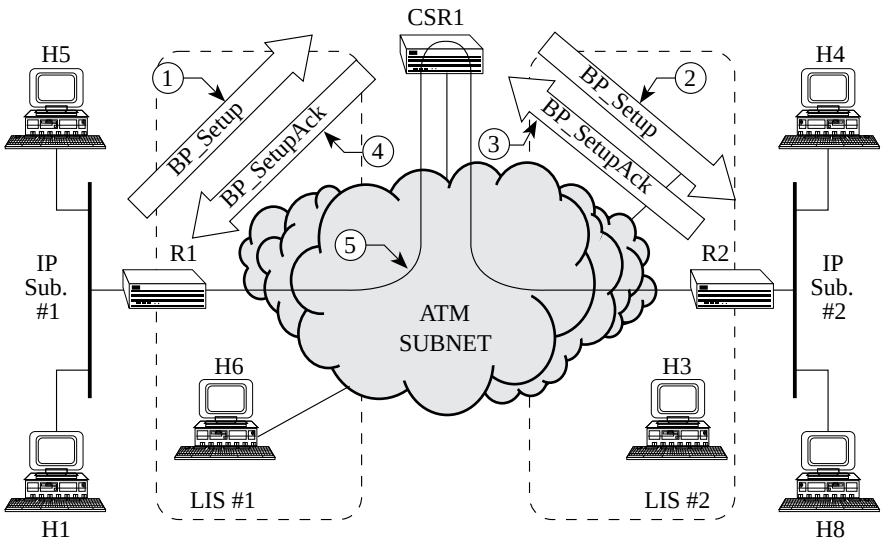


Fig. 21.17 - Esempio di creazione di una ATM bypass-pipe iniziata dal mittente.

Richieste provenienti dalla destinazione

In questo caso, il mittente trasmette periodicamente un messaggio BP_Path verso la destinazione utilizzando il cammino indicato dalla tabella di instradamento (figura 21.18). Tali messaggi sono necessari affinché la destinazione possa inviare i messaggi per la prenotazione delle risorse BP_Resv verso il mittente lungo lo stesso cammino seguito dai messaggi BP_Path. I messaggi BP_Resv sono trasmessi dai nodi (CSR o host) o quando ricevono un messaggio analogo da un nodo più a valle, oppure quando un'entità RSVP al loro interno genera una richiesta di prenotazione.

Il contenuto dei messaggi BP_Resv è lo stesso dei messaggi Resv del protocollo RSVP, con l'aggiunta di informazioni specifiche per la creazione della ATM bypass-pipe come l'identificatore della dedicated-VC da utilizzare come una sua componente e la banda da dedicare ad essa. Quando un nodo riceve un messaggio BP_Resv, determina l'hop precedente mediante le informazioni ricavate dai messaggi BP_Path; se dispone di banda sufficiente ad accogliere la richiesta, seleziona o crea una dedicated-VC verso tale nodo ed infine invia a quest'ultimo un messaggio BP_Resv. Questa procedura viene ripetuta fino a quando il messaggio BP_Resv raggiunge il mittente oppure un CSR intermedio non è in grado di propagare ulteriormente detto messaggio. In quest'ultimo frangente il CSR viene assunto come punto di ingresso della ATM bypass-pipe.

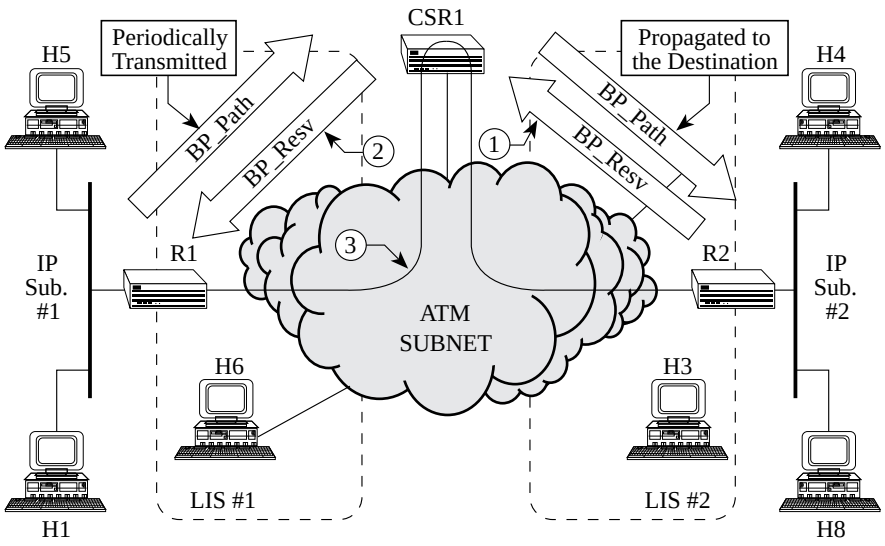


Fig. 21.18 - Esempio di creazione di una ATM bypass-pipe iniziata dalla destinazione.

Dopo la creazione della ATM bypass-pipe, il mittente continua a trasmettere periodicamente messaggi BP_Path così come la destinazione continua l'invio di messaggi BP_Resv. Ciò avviene al fine di mantenere attiva la ATM bypass-pipe: infatti, se anche uno solo dei CSR da questa attraversati non riceve per un certo periodo di tempo un messaggio BP_Resv, provvede automaticamente al suo rilascio.

Qualora si verificasse una variazione nel forwarding IP dovuta a mutamenti topologici durante il periodo di vita di una ATM bypass-pipe, i messaggi BP_Path seguirebbero un nuovo percorso. Automaticamente i corrispondenti messaggi BP_Resv percorrerebbero a ritroso il nuovo cammino, provocando il rilascio della ATM bypass-pipe che seguiva il vecchio percorso e la creazione di una nuova ATM bypass-pipe.

21.14 SUPPORTO DI SERVIZI CONNECTION ORIENTED E QOS

Uno dei motivi per cui il Modello IP Classico tende ad utilizzare l'infrastruttura trasmissiva ATM in modo non ottimale risiede nell'impossibilità di sfruttamento della QoS e delle capacità di gestione del traffico tipiche di un ambiente connection oriented quale ATM. Ciò risulta particolarmente svantaggioso se si pensa alla natura estrema-

mente diversificata del traffico IP in funzione del tipo di applicazioni che lo produce.

Vi sono, ad esempio, applicazioni caratterizzate da una durata molto breve e da uno scambio di pacchetti decisamente contenuto, come ping o le query di DNS (*Domain Name Server*). Altre applicazioni, pur avendo una durata relativamente limitata, generano notevoli moli di traffico come, ad esempio, FTP (*File Transfer Protocol*). Altre ancora sono caratterizzate da una durata piuttosto lunga, ma da un numero di pacchetti scambiati molto contenuto (ad esempio le sessioni telnet). Infine vi sono applicazioni (al momento attuale relativamente poche, ma si prevede un forte sviluppo per il futuro) che hanno sia una durata sia un volume di traffico prodotto decisamente elevati (applicazioni multimediali come la videoconferenza).

Le esigenze in termini di tipo di servizio e di QoS manifestate da applicazioni come quelle sopraccitate sono estremamente diversificate. Ad esempio, per una applicazione di videoconferenza sarebbe adeguato un servizio connection oriented basato su una SVC punto-multipunto a larga banda caratterizzata da ritardo basso e costante e da un tasso di perdita relativamente elevato; d'altra parte, per effettuare una query di un DNS risulterebbe appropriato un servizio connectionless basato su router e realizzato con una SVC avente banda trascurabile, ritardo elevato ed un tasso di perdita il più contenuto possibile.

Nell'ottica della QoS, il Modello IP Classico non è in grado di utilizzare in modo flessibile ed adattativo l'infrastruttura trasmissiva ATM. Infatti l'intero traffico in transito tra due host nella stessa LIS deve essere multiplato, mediante incapsulamento LLC/SNAP, su una singola VC caratterizzata da un servizio di tipo "best effort". Ciò implica che tipi di traffico con esigenze estremamente differenti come quelli sopra descritti devono condividere uno canale di comunicazione di qualità non garantita.

Per considerare correttamente la QoS occorre modificare il Modello IP Classico mediante opportune estensioni architetturali che consentano di:

- stabilire tra gli host più VC da destinare al trasporto di traffici di differente natura;
- svincolare la gestione di dette VC dal processo decisionale sulla "localizzazione" delle destinazioni.

Tale approccio è illustrato nei dettagli nel paragrafo seguente.

21.14.1 Gestione delle VC in funzione della QoS

Per offrire servizi di trasporto adeguati a ciascun tipo di traffico, sarebbe opportuno demandare la gestione delle VC direttamente alle applicazioni o, in modo più appropriato, gestire le VC in funzione dei requisiti di QoS richiesti dalle

applicazioni [4]. Risulta infatti evidente che esistono due classi di applicazioni:

- applicazioni le cui esigenze giustificano ampiamente un servizio connection oriented basato su SVC interamente dedicate (videoconferenza, sessioni interattive, file transfer);
- applicazioni per le quali risulterebbe più appropriato un servizio connectionless realizzato con una PVC condivisa verso il router di default. Per questo secondo tipo di applicazioni, infatti, l'overhead associato alla gestione delle SVC risulta eccessivamente penalizzante, soprattutto qualora la durata delle attività sia breve. Sarebbe assurdo, ad esempio, stabilire una SVC per effettuare una query al DNS ed abbatterla subito dopo; risulta invece più economico inviare il pacchetto con la richiesta per il DNS al router e lasciare che questi si occupi di inoltrarla al destinatario.

Un oculato utilizzo delle SVC dedicate e dei router tende sia a ridurre il carico che grava sulla rete ATM a causa delle frequenti attività di segnalazione per la creazione e l'abbattimento di SVC, sia ad eliminare i ritardi dovuti allo stesso motivo; tale politica produce quindi benefici sia per la rete che per le applicazioni. Una situazione simile allo scenario sopra delineato è rappresentata in figura 21.19. Si può notare che un'operazione di file transfer in corso tra gli host H1 e H2 avviene attraverso una SVC dedicata, mentre una interrogazione al DNS (H3) effettuata da un'altra applicazione in esecuzione su H1 viene fatta transitare attraverso il router R1, esattamente come il ping effettuato da H2 nei confronti di H4.

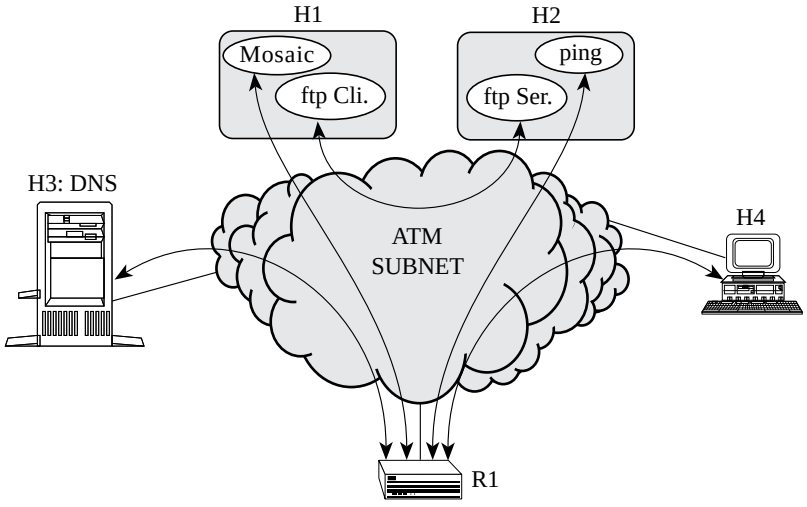


Fig. 21.19 - Esempio di gestione delle VC in funzione della QoS.

In base alla precedente classificazione, ciascun host dovrebbe pertanto stabilire se la destinazioni sono "locali" o "remote" indipendentemente dagli indirizzi IP, ma in funzione delle esigenze di QoS manifestate dalle applicazioni che sta eseguendo. Quindi tale decisione non è più invariante nel tempo. Ad esempio, se l'host H1 esegue ping per verificare se H2 è operativo, la comunicazione passa attraverso il router R1 e la destinazione risulta pertanto "remota". Se, immediatamente dopo aver appurato che H2 è attivo, H1 stabilisce una SVC con H2 per la sessione FTP, la destinazione risulta ora "locale". Inoltre una destinazione può risultare contemporaneamente "locale" e "remota": ad esempio un host che funge da DNS potrebbe operare anche come file server e nessuno impedisce che un altro host possa simultaneamente interrogare il database dei nomi ed effettuare una operazione di file transfer.

21.14.2 Ridefinizione del concetto di LIS

Per permettere che gli host prendano la decisione "destinazione locale/remota" non in base agli indirizzi IP, ma a seconda del tipo di applicazioni che stanno eseguendo, si deve ridefinire il concetto di LIS. Una LIS diviene una associazione tra un insieme di host ed uno o più router che gli host possono utilizzare per raggiungere:

1. destinazioni che non condividono lo stesso Data Link ATM;
2. destinazioni che condividono lo stesso Data Link ATM, ma per le quali non si desidera creare apposite SVC in quanto la comunicazione ha luogo tra applicazioni che non giustificano un tale sforzo.

Dato quindi un insieme di host, una LIS identifica l'insieme di router che gli host possono usare come primo hop (*first-hop router*) verso una delle suddette destinazioni. Dualmente, dato un insieme di router, una LIS identifica l'insieme di host per i quali i router fungono da ultimo hop (*last-hop router*). Tale definizione risulta compatibile con quella del Modello IP Classico su ATM raccomandato dalla RFC 1577, rendendo possibile un percorso di migrazione verso il nuovo modello architetturale assolutamente trasparente. Tale migrazione è realizzabile mediante opportune modifiche agli host ed ai router.

Modifiche agli host

La principale modifica da apportare agli host concerne ovviamente il meccanismo di gestione delle stesse SVC, il quale deve essere posto sotto il controllo

delle applicazioni o, in modo più appropriato, controllato dai requisiti di QoS richiesti dalle applicazioni.

Per ogni applicazione che trarrebbe vantaggi consistenti dall'impiego di una SVC diretta con la controparte, l'host deve tentare di stabilire tale SVC con la destinazione indipendentemente dagli indirizzi IP del mittente e della destinazione. Se non risulta possibile stabilire tale SVC, l'host deve inviare i pacchetti ad un router della LIS (ad esempio il router di default con il quale è tipicamente collegato mediante una PVC o una VC semi-permanente). Per quanto concerne le applicazioni che non traggono benefici dalla connettività diretta, l'host deve rivolgersi in ogni caso ad uno dei router della LIS.

Modifiche ai router

La principale modifica da apportare ai router concerne l'inibizione del meccanismo di redirezione. Quando un router associato ad una LIS riceve un pacchetto da un host appartenente alla LIS e destinato ad un altro host della stessa LIS, esso deve effettuare il forwarding del pacchetto verso l'host di destinazione astenendosi dall'inviare un messaggio ICMP di redirect all'host mittente. Questo in quanto i router di una LIS vengono utilizzati anche per mantenere la connettività nell'ambito della LIS stessa tra host le cui applicazioni non necessitano di SVC dirette.

21.15 ESEMPIO DI INTERFACCIA ATM

Per cercare di fornire un'idea di come possa essere realizzato in pratica quanto sino a qui descritto, questo paragrafo illustra l'organizzazione interna della scheda ATM AIP che è utilizzabile sui router Cisco della famiglia 7000.

La figura 21.20 mostra lo schema a blocchi di tale scheda dove è possibile vedere che sul livello ATM si appoggiano due possibili ALL: l'AAL3/4 e l'AAL5.

Il primo è utilizzato per fornire servizi di tipo SMDS/CBDS quali quelli descritti nel paragrafo 13.6. Lo standard SMDS/CBDS prevede infatti una trasmissione di celle compatibili con quelle ATM; il supporto di più protocolli di livello superiore (in figura 21.20 sono indicati IP, OSI-CLNP, IPX e DDP, ma la lista è incompleta) è fornito tramite un header LLC/SNAP, in accordo allo RFC 1209.

L'AAL5 è invece utilizzato per il Modello IP Classico, per l'emulazione del servizio Frame Relay (si veda il paragrafo 13.5) e per l'emulazione di LAN (si veda il capitolo 20) sia Ethernet sia Token Ring.

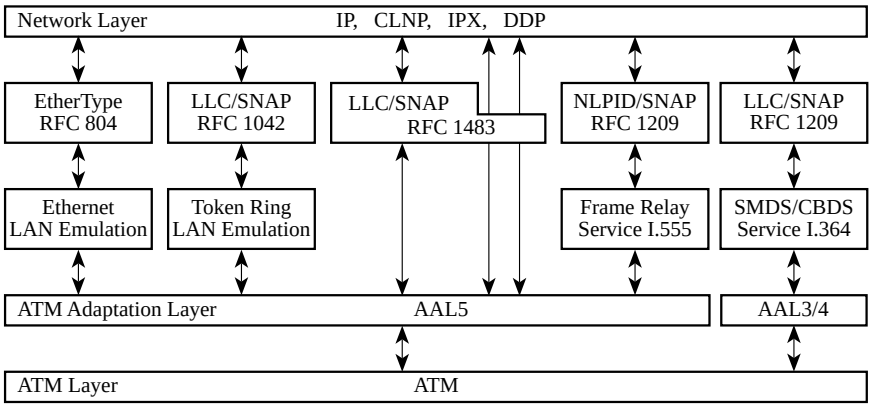


Fig. 21.20 - Schema a blocchi della scheda Cisco AIP.

Il supporto di più protocolli di alto livello può avvenire sia tramite LLC/SNAP, sia tramite null encapsulation e naturalmente tramite LAN Emulation.

La scheda AIP offre sia le funzionalità di LAN Emulation Client sia quelle di LAN Emulation Service; è in grado di operare come ATMARP client e server e gestisce il protocollo NBMA - NHRP sia in versione client sia in versione server.

I livelli fisici supportati dalla scheda sono vari e la scheda è quindi resa disponibile con connettori di interfaccia alternativi. La figura 21.21 dettaglia ulteriormente l'organizzazione di tale scheda con particolare riferimento ai livelli fisici e ATM.

In particolare si può osservare che i livelli fisici sono suddivisi in due gruppi: a trama HDLC e a cella.

Nel caso di interfacce a trama (V.35, HSSI, ...) il protocollo utilizzato è il DXI (si veda il paragrafo 13.6) ed è richiesta una unità di frammentazione in celle (CSU/DSU) esterna.

Nel caso di interfacce a cella sono forniti i seguenti standard:

- plesiocroni in conformità alle gerarchie europee E1, E3 ed E4 ed americane T1 e T3 (si veda il paragrafo 12.5);
- sincroni in conformità alle gerarchie SONET/SDH alle velocità di 155 e 622 Mb/s (si veda il paragrafo 12.6);
- TAXI e ATM nativo su fibra ottica.

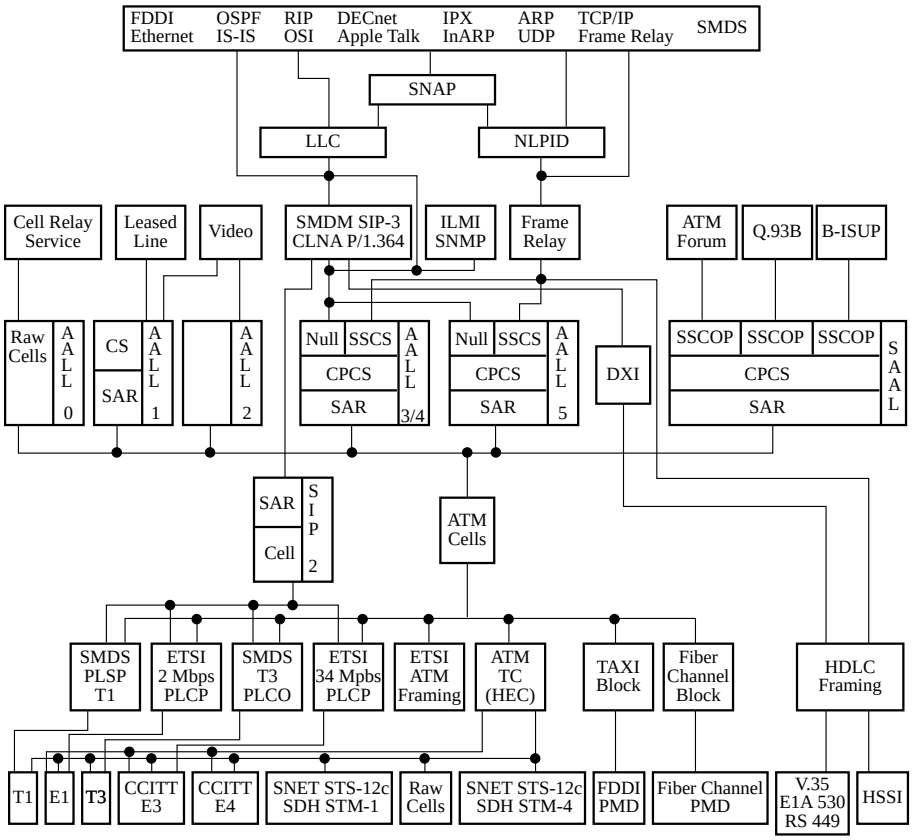


Fig. 21.21 - Schema dettagliato della scheda Cisco AIP.

BIBLIOGRAFIA

[1] R.G Cole, D.H.Shur, C.Villamizar, "IP over ATM: A Framework Document," Internet Draft, draft-ietf-ipatm-framework-doc-02, April 1995.

[2] J. Heinanen, "RFC 1483: Multiprotocolo Encapsulation over ATM adaptation layer 5," July 1993.

[3] R. Braden, J. Postel amd Y. Rekhter, "RFC 1620: Internet Architecture Extensions for Shared Media," May 1994.

[4] Y. Rekhter, D. Kandlur, "IP Architecture Extensions for ATM," Internet Draft draft-rekhter-ip-atm-architecture.txt, January 1995.

[5] Y. Katsube, K. Nagami and H. Esaki, "Router Architecture Extensions for ATM: Overview," Internet Draft draft-katsube-router-atm-overview-00.txt, March 1995.

[6] D. Katz, D. Piscitello, "NBMA Next Hop Resolution Protocol," Internet Draft draft-ietf-rolc-nhrp-04.txt, May 1995.

[7] G. Armitage, "Support for multicast over UNI 3.1 based ATM networks," Internet Draft draft-ietf- ipatm-ipmc-04.txt, February 1995.

[8] R. Atkinson, "RFC 1626: Default IP MTU for use over ATM AAL5," May 1994.

[9] ATM Forum, "ATM User-Network Interface Specification," Prentice Hall, September 1993.

[10] J. Garrett, J. Hagan, and J. Wong, "RFC 1433: Directed ARP," March 1993.

[11] J. Heinanen and R. Govindan, "RFC 1735: NBMA address resolution protocol (NARP)," December 1994.

[12] M. Laubach, "RFC 1577: Classical IP and ARP over ATM," January 1994.

[13] J. Mogul and S. Deering. "RFC 1191: Path MTU discovery," November 1990.

[14] M. Perez, F. Liaw, D. Grossman, A. Mankin, and A. Hoffman, "RFC 1755: ATM signalling support for IPover ATM," January 1995.

[15] M. Ohta et al., "Connection Oriented and Connectionless IP Forwarding over ATM networks", Internet Draft, October 1994

Appendice A

PRINCIPALI CODIFICHE

Questa appendice riporta alcune tabelle contenenti i principali identificativi di protocollo che è comune trovare sulle LAN. Essa è principalmente ricavata dallo standard RFC 1340 "Assigned Number". Molto spesso esistono incertezze o ambiguità su alcune assegnazioni e queste vengono evidenziate con il simbolo "?". Inoltre il simbolo "x" indica una quasiasi cifra esadecimale.

A.1 IEEE 802.2 SAP

Sono i valori che si possono trovare contenuti nei campi DSAP e SSAP del pacchetto LLC. I SAP LLC sono grandi un byte e hanno due bit con un significato particolare, come descritto in figura 5.9. Esistono due tipi di LLC SAP, quelli definiti dall'IEEE e quelli assegnati localmente.

A.1.1 LLC SAP definiti dall'IEEE

Per ottenere l'assegnazione di un LLC SAP standard occorre contattare lo IEEE Standards Office, 345 East 47th Street, New York, N.Y. 10017, USA, Attn: Vince Condello. Phone: (212) 705-7092.

Quelli ufficialmente definiti sono elencati in tabella A.1.

Esadecimale	Significato
00	Null LSAP
02	Individual LLC Sublayer Management
x2	Network Management Function
03	Group LLC Sublayer Management
x6	National Body Standard
06	DOD IP
0E	PROWAY-LAN
42	IEEE 802.1D (MAC bridge)
4E	EIA-RS 511
5E	ISI IP
8E	PROWAY-LAN
AA	SNAP
FE	ISO CLNS
FF	Global DSAP

Tab. A.1 - LLC SAP definiti dall'IEEE.

A.1.2 LLC SAP definiti dagli utenti

La tabella A.2 riporta alcuni LLC SAP definiti da IBM.

Esadecimale	Significato
04	SNA Path Control
05	SNA Path Control Group
F0	IBM Netbios
F4	LAN Management Individual
F5	LAN Management Group

Tab. A.2 - LLC SAP definiti dagli utenti.

A.2 ETHERNET PROTOCOL TYPE

Sono assegnati dalla Xerox. Se avete necessità di ottenere un Protocol Type ufficiale per un vostro protocollo proprietario contattate la Xerox Corporation, Xerox Systems Institute, 475 Oakmead Parkway, Sunnyvale, CA 94086, USA, Attn: Ms. Fonda Pallone, Phone (415) 813-7164. La tabella A.3 riporta una lista aggiornata a Luglio 1992.

0000-05DC	IEEE802.3 Length Field
0600	XEROX NS IDP
0800	DOD IP
0801	X.75 Internet
0802	NBS Internet
0803	ECMA Internet
0804	Chaosnet
0805	X.25 Level 3
0806	ARP
0807	XNS Compatability
081C	Symbolics Private
0888	Xyplex
0900	Ungermann-Bass net debuger
0A00	Xerox IEEE802.3 PUP
0A01	PUP Addr Trans
0BAD	Banyan Systems
1000	Berkeley Trailer nego
1001-100F	Berkeley Trailer enca
1600	Valid Systems
4242	PCS Basic Block Proto
5208	BBN Simnet
6000	DEC Unassigned (Exp.)
6001	DEC MOP Dump/Load
6002	DEC MOP Remote Consol
6003	DEC DECNET Phase IV R
6004	DEC LAT
6005	DEC Diagnostic Protocol
6006	DEC Customer Protocol
6007	DEC LAVC SCA
6008-6009	DEC Unassigned
6010	3Com Corporation
7000	Ungermann-Bass download
7002	Ungermann-Bass dia/loop
7020-7029	LRT
7030	Proteon
7034	Cabletron
8003	Cronus VLN
8004	Cronus Direct
8005	HP Probe
8006	Nestar
8008	AT&T
8010	Excelan
8013	SGI diagnostics
8014	SGI network games
8015	SGI reserved
8016	SGI bounce server
8019	Apollo Computers
802E	Tymshare
802F	Tigan Inc.
8035	Reverse ARP
8036	Aeonic Systems
8038	DEC LANBridge
8039	DEC Unassigned
803D	DEC Ethernet Encryption
803E	DEC Unassigned
803F	DEC LAN Traffic Monitor
8040-8042	DEC Unassigned
8044	Planning Research Corp.
8046	AT&T
8047	AT&T
8049	ExperData
805B	Stanford V Kernel experimental
805C	Stanford V Kernel production
805D	Evans & Sutherland
8060	Little Machines
8062	Counterpoint Computers
8065-8066	Univ. of Mass. @ Amherst
8067	Veeco Integrated Auto
8068	General Dynamics
8069	AT&T

806A	Autophon
806C	ComDesign
806D	Computgraphic Corp.
806E-8077	Landmark Graphics Corp.
807A	Matra
807B	Dansk Data Elektronik
807C	Merit Internodal
807D-807F	Vitalink Communications
8080	Vitalink TransLAN III
8081-8083	Counterpoint Computers
809B	Appletalk
809C-809E	Datability
809F	Spider Systems Ltd.
80A3	Nixdorf Computers
80A4-80B3	Siemens Gammasonics Inc.
80C0-80C3	DCA Data Exchange Cluster
80C6	Pacer Software
80C7	Applitek Corporation
80C8-80CC	Intergraph Corporation
80CD-80CE	Harris Corporation
80CF-80D2	Taylor Instrument
80D3-80D4	Rosemount Corporation

80D5	IBM SNA Service on Et
80DD	Varian Associates
80DE-80DF	Integrated Solutions TRFS
80E0-80E3	Allen-Bradley
80E4-80F0	Datability
80F2	Retix
80F3	AppleTalk AARP (Kinet
80F4-80F5	Kinetics
80F7	Apollo Computer
80FF-8103	Wellfleet Communications
8107-8109	Symbolics Private
8130	Waterloo Microsystems
8131	VG Laboratory Systems
8137-8138	Novell Inc.
8139-813D	KTI
814C	SNMP
9000	Loopback
9001	3Com(Bridge) XNS System Mangement
9002	3Com(Bridge) TCP-IP System Management
9003	3Com(Bridge) loop detetction
FF00	BBN VITAL-LanBridge cache

Tab. A.3 - Ethernet Protocol Type.

A.3 OUI: ORGANIZATION UNIQUE IDENTIFIER

Gli OUI detti anche "Vendor Code" sono i lotti di indirizzi MAC 802 assegnati dalla IEEE. Il formato di un indirizzo MAC è su 48 bit di cui i primi 24 (6 cifre esadecimali) rappresentano l'OUI.

I due bit meno significativi del primo byte hanno un significato particolare (si veda il paragrafo 5.6.7).

Gli OUI si richiedono all'IEEE Standards Office, 345 East 47th Street, New York, N.Y. 10017, USA, Attn: Vince Condello. Phone: (212) 705-7092.

Quelli attualmente assegnati sono riportati in tabella A.4.

00-00-0C	Cisco	
00-00-0F	NeXT	
00-00-10	Sytek	
00-00-1D	Cabletron	
00-00-20	DIAB (Data Intdustrier AB)	
00-00-22	Visual Technology	
00-00-2A	TRW	
00-00-5A	S & Koch	
00-00-5E	IANA	
00-00-65	Network General	
00-00-6B	MIPS	
00-00-77	MIPS	
00-00-7A	Ardent	
00-00-89	Cayman Systems	Gatorbox
00-00-93	Proteon	
00-00-9F	Ameristar Technology	
00-00-A2	Wellfleet	
00-00-A3	Network Application Technology	
00-00-A6	Network General	internal use
00-00-A7	NCD	X-terminals
00-00-A9	Network Systems	
00-00-AA	Xerox	Xerox machines
00-00-B3	CIMLinc	
00-00-B7	Dove	Fastnet
00-00-BC	Allen-Bradley	
00-00-C0	Western Digital	
00-00-C6	HP	Intelligent Networks Operation
00-00-C8	Altos	
00-00-C9	Emulex	Terminal Servers
00-00-D7	Dartmouth College	NED Router
00-00-D8	3Com? Novell? PS/2	
00-00-DD	Gould	
00-00-DE	Unigraph	
00-00-E2	Acer Counterpoint	
00-00-EF	Alantec	
00-00-FD	High Level Hardvare	Orion (UK)
00-01-02	BBN	internal usage
00-17-00	Kabel	
00-80-2D	Xylogics Inc.	Annex terminal servers
00-80-8C	Frontier Software Development	
00-80-C2	IEEE 802.1 Committee	
00-80-D3	Shiva	
00-AA-00	Intel	

00-DD-00	Ungermann-Bass	
00-DD-01	Ungermann-Bass	
02-07-01	Racal InterLan	
02-04-06	BBN	internal usage
02-60-86	Satelcom MegaPac (UK)	
02-60-8C	3Com	IBM PC; Imagen; Valid; Cisco
02-CF-1F	CMC	Masscomp; Silicon Graphics; Prime EXL
08-00-02	3Com	Formerly Bridge
08-00-03	Advanced Computer Communications	
08-00-05	Symbolics	Symbolics LISP machines
08-00-07	Apple	
08-00-08	BBN	
08-00-09	Hewlett-Packard	
08-00-0A	Nestar Systems	
08-00-0B	Unisys	
08-00-11	Tektronix	Inc.
08-00-14	Excelan	BBN Butterfly, Masscomp, Silicon Graphics
08-00-17	NSC	
08-00-1A	Data General	
08-00-1B	Data General	
08-00-1E	Apollo	
08-00-20	Sun	Sun machines
08-00-22	NBI	
08-00-25	CDC	
08-00-26	Norsk Data	
08-00-27	PCS Computer Systems	
08-00-28	TI	Explorer
08-00-2B	DEC	
08-00-2E	Metaphor	
08-00-2F	Prime Computer	Prime 50-Series
08-00-36	Intergraph	CAE stations
08-00-37	Fujitsu-Xerox	
08-00-38	Bull	
08-00-39	Spider Systems	
08-00-41	Digital Comm. Assoc.	
08-00-46	Sony	
08-00-47	Sequent	
08-00-49	Univation	
08-00-4C	Encore	
08-00-4E	BICC	
08-00-56	Stanford University	
08-00-5A	IBM	
08-00-67	Comdesign	
08-00-68	Ridge	

08-00-69	Silicon Graphics	
08-00-6E	Excelan	
08-00-75	Danish Data Elektronik	
08-00-7C	Vitalink	TransLAN III
08-00-80	XIOS	
08-00-86	Imagen/QMS	
08-00-87	Xyplex	terminal servers
08-00-89	Kinetics	AppleTalk-Ethernet interface
08-00-8B	Pyramid	
08-00-8D	XyVision	XyVision machines
08-00-90	Retix Inc	Bridges
48-44-53	HDS ???	
80-00-10	AT&T	
AA-00-00	DEC	obsolete
AA-00-01	DEC	obsolete
AA-00-02	DEC	obsolete
AA-00-03	DEC	Global physical address for some DEC machines
AA-00-04	DEC	Local logical address for systems running DECNET

Tab. A.4 - Organization Unique Identifier.

A.4 INDIRIZZI MAC MULTICAST

La tabella A.5 contiene indirizzi di multicast assegnati a vari enti. La seconda colonna identifica, se esiste, il protocol type che utilizza il multicast.

01-00-5E-00-00-00	0800	Internet Multicast (RFC-1112), sino a
01-00-5E-7F-FF-FF	0800	
01-00-5E-80-00-00		Internet reserved by IANA, sino a
01-00-5E-FF-FF-FF		
01-80-C2-00-00-00		802 Spanning tree for bridges
09-00-02-04-00-01?	8080?	Vitalink printer
09-00-02-04-00-02?	8080?	Vitalink management
09-00-09-00-00-01	8005	HP Probe
09-00-09-00-00-01		HP Probe
09-00-09-00-00-04	8005?	HP DTC
09-00-1E-00-00-00	8019?	Apollo DOMAIN

09-00-2B-00-00-00	6009?	DEC MUMPS?
09-00-2B-00-00-01	8039?	DEC DSM/DTP?
09-00-2B-00-00-02	803B?	DEC VAXELN?
09-00-2B-00-00-03	8038	DEC Lanbridge Traffic Monitor (LTM)
09-00-2B-00-00-04		DEC MAP End System Hello
09-00-2B-00-00-05		DEC MAP Intermediate System Hello
09-00-2B-00-00-06	803D?	DEC CSMA/CD Encryption?
09-00-2B-00-00-07	8040?	DEC NetBios Emulator?
09-00-2B-00-00-0F	6004	DEC Local Area Transport (LAT)
09-00-2B-00-00-1x		DEC Experimental
09-00-2B-01-00-00	8038	DEC LanBridge Copy packets (All bridges)
09-00-2B-01-00-01	8038	DEC LanBridge Hello packets (All local bridges)
09-00-2B-02-00-00		DEC DNA Lev. 2 Routing Layer routers?
09-00-2B-02-01-00	803C?	DEC DNA Naming Service Advertisement?
09-00-2B-02-01-01	803C?	DEC DNA Naming Service Solicitation?
09-00-2B-02-01-02	803E?	DEC DNA Time Service?
09-00-2B-03-xx-xx		DEC default filtering by bridges?
09-00-2B-04-00-00	8041?	DEC Local Area Sys. Transport (LAST)?
09-00-2B-23-00-00	803A?	DEC Argonaut Console?
09-00-4E-00-00-02	8137?	Novell IPX
09-00-56-00-00-00		Stanford reserved, sino a
09-00-56-FE-FF-FF		
09-00-56-FF-00-00	805C	Stanford V Kernel, version 6.0, sino a
09-00-56-FF-FF-FF		
09-00-77-00-00-01		Retix spanning tree bridges
09-00-7C-02-00-05	8080?	Vitalink diagnostics
09-00-7C-05-00-01	8080?	Vitalink gateway?
0D-1E-15-BA-DD-06		HP
AB-00-00-01-00-00	6001	DEC Maintenance Operation Protocol (MOP)
09-00-09-00-00-01		HP Probe
09-00-09-00-00-04	8005?	HP DTC
09-00-1E-00-00-00	8019?	Apollo DOMAIN
09-00-2B-00-00-00	6009?	DEC MUMPS?
09-00-2B-00-00-01	8039?	DEC DSM/DTP?
09-00-2B-00-00-02	803B?	DEC VAXELN?
09-00-2B-00-00-03	8038	DEC Lanbridge Traffic Monitor (LTM)

09-00-2B-00-00-04		DEC MAP End System Hello
09-00-2B-00-00-05		DEC MAP Intermediate System Hello
09-00-2B-00-00-06	803D?	DEC CSMA/CD Encryption?
09-00-2B-00-00-07	8040?	DEC NetBios Emulator?
09-00-2B-00-00-0F	6004	DEC Local Area Transport (LAT)
09-00-2B-00-00-1x		DEC Experimental
09-00-2B-01-00-00	8038	DEC LanBridge Copy packets (All bridges)
09-00-2B-01-00-01	8038	DEC LanBridge Hello packets (All local bridges)
09-00-2B-02-00-00		DEC DNA Lev. 2 Routing Layer routers?
09-00-2B-02-01-00	803C?	DEC DNA Naming Service Advertisement?
09-00-2B-02-01-01	803C?	DEC DNA Naming Service Solicitation?
09-00-2B-02-01-02	803E?	DEC DNA Time Service?
09-00-2B-03-xx-xx		DEC default filtering by bridges?
09-00-2B-04-00-00	8041?	DEC Local Area Sys. Transport (LAST)?
09-00-2B-23-00-00	803A?	DEC Argonaut Console?
09-00-4E-00-00-02	8137?	Novell IPX
09-00-56-00-00-00		Stanford reserved, sino a
09-00-56-FE-FF-FF		
09-00-56-FF-00-00	805C	Stanford V Kernel, version 6.0, sino a
09-00-56-FF-FF-FF		
09-00-77-00-00-01		Retix spanning tree bridges
09-00-7C-02-00-05	8080?	Vitalink diagnostics
09-00-7C-05-00-01	8080?	Vitalink gateway?
0D-1E-15-BA-DD-06		HP
AB-00-00-01-00-00	6001	DEC Maintenance Operation Protocol (MOP)
AB-00-00-02-00-00	6002	DEC MOP Remote Console
AB-00-00-03-00-00	6003	DECNET Phase IV end node Hello
AB-00-00-04-00-00	6003	DECNET Phase IV Router Hello packets
AB-00-00-05-00-00		Reserved DEC sino a
AB-00-03-FF-FF-FF		
AB-00-03-00-00-00	6004	DEC Local Area Transport (LAT) - old
AB-00-04-00-xx-xx		Reserved DEC customer private use
AB-00-04-01-xx-yy	6007	DEC Local Area VAX Cluster groups
CF-00-00-00-00-00	9000	Ethernet Configuration Test protocol (Loopback)

Tab. A.5 - MAC Multicast.

A.5 INDIRIZZI IP

Ci sono cinque classi di indirizzi IP: dalla classe A alla classe E. La classe E è riservata ad usi sperimentali. Ci sono alcuni casi particolari per gli indirizzi IP che sono discussi nel seguito. La notazione usata è:

IP-address ::= { <Network-number>, <Host-number> }

oppure

IP-address ::= {<Network-number>,<Subnet-number>, <Host-number> }.

Inoltre il valore "-1" indica un campo di tutti uno.

I casi speciali sono riportati nella tabella A.6.

{0,0}	Questo calcolatore su questa Net
{0, <Host-num>}	Questo calcolatore su questa Net
{ -1, -1}	Broadcast limitato alla (Sub-)Net mittente
{<Network-num>, -1}	Broadcast verso una data Net
{<Network-num>, <Subnet-num>, -1}	Broadcast verso una data Subnet
{<Network-num>, -1, -1}	Broadcast verso tutte le subnet di una net
{127, <any>}	Internal host loopback address.

Tab. A.6 - Indirizzi IP speciali.

A.6 INTERNET MULTICAST ADDRESSES

Lo standard RFC 1112 descrive le estensioni per l'implementazione del multicasting su IP.

Questi indirizzi sono elencati nel Domain Name Service sotto MCAST.NET and 224.IN-ADDR.ARPA.

Gli indirizzi considerati sono riportati nella tabella A.7.

224.0.0.0	Reserved
224.0.0.1	All Systems on this Subnet
224.0.0.2	All Routers on this Subnet
224.0.0.3	Unassigned
224.0.0.4	DVMRP Routers
224.0.0.5	OSPFIGP OSPFIGP All Routers
224.0.0.6	OSPFIGP OSPFIGP Designated Routers
224.0.0.7	ST Routers
224.0.0.8	ST Hosts
224.0.0.9	RIP2 Routers
224.0.0.10-224.0.0.255	Unassigned
224.0.1.0	VMTP Managers Group
224.0.1.1	NTP Network Time Protocol
224.0.1.2	SGI-Dogfight
224.0.1.3	Rwhod
224.0.1.4	VNP
224.0.1.5	Artificial Horizons - Aviator
224.0.1.6	NSS - Name Service Server
224.0.1.7	AUDIONEWS - Audio News Multicast
224.0.1.8	SUN NIS+ Information Service
224.0.1.9	MTP Multicast Transport Protocol
224.0.1.10-224.0.1.255	Unassigned
224.0.2.1	"rwho" Group (BSD) (unofficial)
224.0.2.2	SUN RPC PMAPPROC_CALLIT
224.0.3.0-224.0.3.255	RFE Generic Service
224.0.4.0-224.0.4.255	RFE Individual Conferences
224.1.0.0-224.1.255.255	ST Multicast Groups
224.2.0.0-224.2.255.255	Multimedia Conference Calls
232.x.x.x	VMTP transient groups

Tab. A.7 - Indirizzi Internet Multicast.

A.7 IP PROTOCOL NUMBERS

Nel protocollo IP esiste un campo detto "Protocol" per identificare quale protocollo è contenuto nel campo INFO del pacchetto IP.

I valori assegnati a tale campo sono riportati nella tabella A.8.

0		Reserved
1	ICMP	Internet Control Message
2	IGMP	Internet Group Management
3	GGP	Gateway-to-Gateway
4	IP	IP in IP (encasulation)
5	ST	Stream
6	TCP	Transmission Control
7	UCL	UCL
8	EGP	Exterior Gateway Protocol
9	IGP	any private interior gateway
10	RCC-MON	BBN RCC Monitoring
11	NVP-II	Network Voice Protocol
12	PUP	PUP
13	ARGUS	ARGUS
14	EMCON	EMCON
15	XNET	Cross Net Debugger
16	CHAOS	Chaos
17	UDP	User Datagram Protocol
18	MUX	Multiplexing
19	DCN-MEAS	DCN Measurement Subsystems
20	HMP	Host Monitoring
21	PRM	Packet Radio Measurement
22	XNS-IDP	XEROX NS IDP
23	TRUNK-1	Trunk-1
24	TRUNK-2	Trunk-2
25	LEAF-1	Leaf-1
26	LEAF-2	Leaf-2
27	RDP	Reliable Data Protocol
28	IRTP	Internet Reliable Transaction
29	ISO-TP4	ISO Transport Protocol Class 4
30	NETBLT	Bulk Data Transfer Protocol
31	MFE-NSP	MFE Network Services Protocol
32	MERIT-INP	MERIT Internodal Protocol
33	SEP	Sequential Exchange Protocol
34	3PC	Third Party Connect Protocol
35	IDPR	Inter-Domain Policy Routing Protocol
36	XTP	XTP
37	DDP	Datagram Delivery Protocol
38	IDPR-CMTP	IDPR Control Message Transport Protol
39	TP++	TP++ Transport Protocol
40	IL	IL Transport Protocol
41-60		Unassigned
61		any host internal protocol

62	CFTP	CFTP
63		any local network
64	SAT-EXPAK	SATNET and Backroom EXPAK
65	KRYPTOLAN	Kryptolan
66	RVD	MIT Remote Virtual Disk Protocol
67	IPPC	Internet Pluribus Packet Core
68		any distributed file system
69	SAT-MON	SATNET Monitoring
70	VISA	VISA Protocol
71	IPCV	Internet Packet Core Utility
72	CPNX	Computer Protocol Network Executive
73	CPHB	Computer Protocol Heart Beat
74	WSN	Wang Span Network
75	PVP	Packet Video Protocol
76	BR-SAT-MON	Backroom SATNET Monitoring
77	SUN-ND	SUN ND PROTOCOL-Temporary
78	WB-MON	WIDEBAND Monitoring
79	WB-EXPAK	WIDEBAND EXPAK
80	ISO-IP	ISO Internet Protocol
81	VMTP	VMTP
82	SECURE-VMTP	SECURE-VMTP
83	VINES	VINES
84	TTP	TTP
85	NSFNET-IGP	NSFNET-IGP
86	DGP	Dissimilar Gateway Protocol
87	TCF	TCF
88	IGRP	IGRP
89	OSPFIGP	OSPFIGP
90	Sprite-RPC	Sprite RPC Protocol
91	LARP	Locus Address Resolution Protocol
92	MTP	Multicast Transport Protocol
93	AX.25	AX.25 Frames
94	IPIP	IP-within-IP Encapsulation Protocol
95	MICP	Mobile Internetworking Control Pro.
96	AES-SP3-D	AES Security Protocol 3-D
97	ETHERIP	Ethernet-within-IP Encapsulation
98	ENCAP	Encapsulation Header
99-254		Unassigned
255		Reserved

Tab. A.8 - Possibili valori del campo IP Protocol.

A.8 PPP DLL PROTOCOL NUMBER

Il protocollo PPP (Point-to-Point Protocol) contiene un Protocol Field lungo 16 bit utilizzato per identificare a quale protocollo appartiene il pacchetto incapsulato.

I valori nell'intervallo da 0xxx a 3xxx identificano il protocollo di livello network, mentre i valori da 8xxx a Bxxx identificano i datagram appartenenti al Network Control Protocol (NCP) associato, se esistente.

La tabella A.9 riporta i valori attualmente assegnati.

0001 to 001f	reserved (transparency inefficient)
0021	Internet Protocol
0023	OSI Network Layer
0025	Xerox NS IDP
0027	DECnet Phase IV
0029	Appletalk
002b	Novell IPX
002d	Van Jacobson Compressed TCP/IP
002f	Van Jacobson Uncompressed TCP/IP
0031	Bridging PDU
0033	Stream Protocol (ST-II)
0035	Banyan Vines
0037	reserved (until 1993)
00ff	eserved (compression inefficient)
0201	802.1d Hello Packets
0231	Luxcom
0233	Sigma Network Systems
8021	Internet Protocol Control Protocol
8023	OSI Network Layer Control Protocol
8025	Xerox NS IDP Control Protocol
8027	DECnet Phase IV Control Protocol
8029	Appletalk Control Protocol
802b	Novell IPX Control Protocol
802d	Reserved
802f	Reserved
8031	Bridging NCP
8033	Stream Protocol Control Protocol
8035	Banyan Vines Control Protocol
8037	reserved till 1993
80ff	reserved (compression inefficient)
c021	Link Control Protocol
c023	Password Authentication Protocol
c025	Link Quality Report
c223	Challenge Handshake Authentication Protocol

Tab. A.9 - PPP DLL Protocol Number.

A.9 ADDRESS RESOLUTION PROTOCOL

Il protocollo ARP ha diversi parametri di cui i due principali sono: Operation Code (tab. A.10) e l'Hardware Type (tab. A.11).

1	REQUEST
2	REPLY

Tab. A.10 - ARP Operation Code.

1	Ethernet (10Mb)
2	Experimental Ethernet (3Mb)
3	Amateur Radio AX.25
4	Proteon ProNET Token Ring
5	Chaos
6	IEEE 802 Networks
7	ARCNET
8	Hyperchannel
9	Lanstar
10	Autonet Short Address
11	LocalTalk
12	LocalNet (IBM PCNet or SYTEK LocalNET)
13	Ultra link
14	SMDS
15	Frame Relay
16	Asynchronous Transmission Mode (ATM)

Tab. A.11 - ARP Hardware Type.

A.10 X.25 TYPE NUMBERS

IL CCITT ha definito i due bit più significativi del campo "Call User Data" nel modo descritto in tabella A.12.

00	Used for other CCITT recommendations (such as X.29)
01	Reserved for use by "national" administrative authorities
10	Reserved for use by international administrative authorities
11	Reserved for arbitrary use between consenting DTEs

Tab. A.12 - Bit MSB di CUD.

Ha inoltre definito i valori di CUD riportati in tabella A.13.

01	PAD
C5	Blacker front-end descr dev
CC	IP
CD	ISO-IP
DD	Network Monitoring

Tab. A.13 - Valori di CUD.

BIBLIOGRAFIA

[1] J. Reynolds, J. Postel, "RFC 1340: Assigned Nuber", July 1992.

[2] IBM, "Token-Ring Network: Architecture Reference", Pub. No. SC30-3374-01, second edition, August 1987.

Appendice B

ESEMPI DI PDU

Questa appendice contiene una serie di pacchetti catturati da diverse reti locali con un analizzatore di protocollo Sniffer v.3.0 della Network General. L'analizzatore è stato programmato per fornire la decodifica dei vari protocolli a partire dai livelli più alti del modello di riferimento OSI, sino a giungere al livello 2 (Data Link), oltre che il pacchetto in esadecimale.

B.1 ESEMPIO DI DECODIFICA

La figura B.1 rappresenta un pacchetto LLC di tipo supervisory frame. Il pacchetto ha unicamente la busta 802.3 e la busta 802.2. I primi 6 byte del pacchetto contengono l'indirizzo di destinazione a livello MAC (MAC-DSAP) e i secondi 6 byte l'indirizzo di mittente a livello MAC (MAC-SSAP).

I due byte che seguono possono essere interpretati come protocol type (nel caso che il pacchetto sia Ethernet, e allora il valore contenuto deve essere maggiore di 1500) oppure come length (nel caso che il pacchetto sia 802.3, e allora il valore contenuto deve essere minore uguale a 1500). In questo caso il valore è 4 quindi si tratta di un pacchetto 802.3 e il significato è length.

Segue il pacchetto LCC che ha LLC-DSAP e LLC-SSAP uguali a 4. Tale valore indica dei SAP LLC di tipo user defined ed in particolare la codifica 4 indica che si tratta di un pacchetto di SNA Path Control.

Segue il campo control che nei pacchetti di tipo supervisory è su due byte (se si fosse trattato di un pacchetto unnumbered sarebbe stato su un byte solo).

Non vi sono dati trattandosi di un supervisory frame.

Il pacchetto non raggiunge la dimensione minima di 64 byte richiesta per la

trasmissione su 802.3 e quindi vengono aggiunti 42 byte di padding.

Analizzando più nel dettaglio il campo control, vediamo che si tratta di un supervisory frame di sottotipo receiver ready (RR), che trasporta un NAK per il pacchetto numero 92.

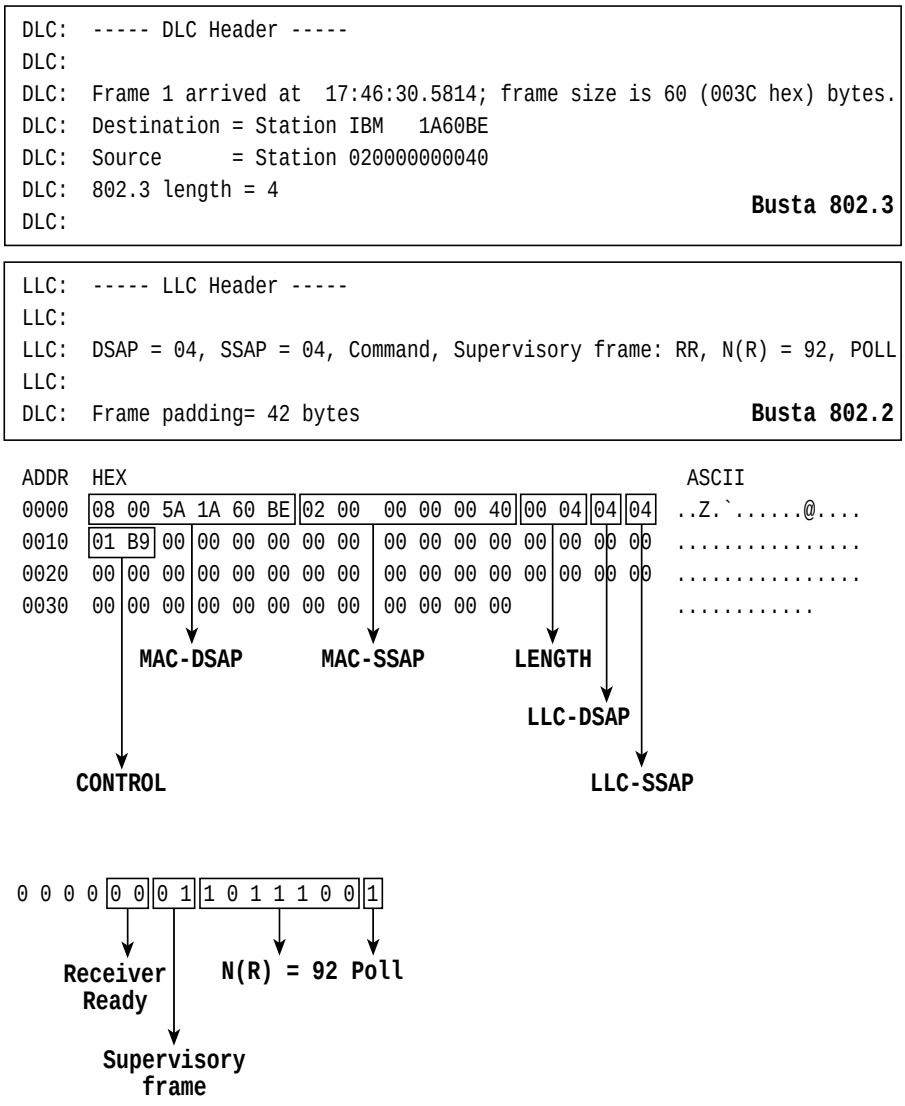

DLC: ----- DLC Header -----
DLC:
DLC: Frame 1 arrived at 17:46:30.5814; frame size is 60 (003C hex) bytes.
DLC: Destination = Station IBM 1A60BE
DLC: Source = Station 020000000040
DLC: 802.3 length = 4
DLC:
Busta 802.3
LLC: ----- LLC Header -----
LLC:
LLC: DSAP = 04, SSAP = 04, Command, Supervisory frame: RR, N(R) = 92, POLL
LLC:
DLC: Frame padding= 42 bytes
Busta 802.2
ADDR HEX ASCII
0000 08 00 5A 1A 60 BE 02 00 00 00 00 40 00 04 04 04 ..Z.`.....@....
0010 01 B9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0030 00 00 00 00 00 00 00 00 00 00 00 00 ....
MAC-DSAP
MAC-SSAP
LENGTH
LLC-DSAP
CONTROL
LLC-SSAP
0 0 0 0 0 0 0 1 1 0 1 1 1 0 0 1
Receiver Ready
N(R) = 92 Poll
Supervisory frame

Fig. B.1 - Esempio di decodifica.

B.2 IBM

In questo sottoparagrafo sono riportati alcuni pacchetti appartenenti all'architettura di rete IBM SNA.

B.2.1 SNA

Il pacchetto seguente è un pacchetto di bind di una sessione SNA di tipo LU 6.2, imbustato in un pacchetto SNA path control, imbustato in un pacchetto LLC di tipo information (LLC connesso o di tipo 2), imbustato in un pacchetto 802.3 con un campo dati di 94 byte.

```
DLC:  Destination = Station IBM   1A60BE
DLC:  Source      = Station 020000000040
DLC:  802.3 length = 94
DLC:
LLC:  ----- LLC Header -----
LLC:
LLC:  DSAP = 04, SSAP = 04, Command, I frame, N(R) = 92, N(S) = 34
LLC:
SNA:  ----- SNA Transmission Header -----
SNA:
SNA:  Format identification (FID) = 2
SNA:
SNA:  Header flags = 2F
SNA:     0010 .... = Format identification
SNA:     .... 11.. = Only segment
SNA:     .... ..1. = Address field negotiation flag
SNA:     .... ...1 = Expedited flow
SNA:  Destination address = 01
SNA:  Origin      address = 01
SNA:  Sequence number = 0
SNA:
SNA:  ----- SNA Request Header (RH) -----
SNA:
SNA:  RH byte 0           = 6B
SNA:            0... .... = Command
SNA:            .11. .... = RU category is 'session control'
SNA:            .... 1... = FM or NS header follows
SNA:            .... .0.. = Sense data not included
SNA:            .... ..11 = Only RU in chain
SNA:  RH byte 1           = 80
SNA:            1.00 .... = Definite response requested
SNA:            .... ..0. = Response bypasses TC queues
SNA:            .... ...0 = Pacing indicator
```

```
SNA:  RH byte 2           = 00
SNA:            0... .... = Begin bracket indicator
SNA:            .0.. .... = End bracket indicator
SNA:            .... ...0 = Conditional end bracket indicator
SNA:            ..0. .... = Change direction indicator
SNA:            .... 0... = Character code selection indicator
SNA:            .... .0.. = Enciphered data indicator
SNA:            .... ..0. = Padded data indicator
SNA:
SNA:  ----- SNA SC-RU (Session Control) -----
SNA:
SNA:  SC code = 31 (BIND: Bind Session)
SNA:  Type = 0 (Negotiable)
SNA:  FM profile = 19
SNA:  TS profile = 7
SNA:  Primary   flags = B0
SNA:        1... .... = Multiple RU chains allowed
SNA:        .0.. .... = Immediate request mode
SNA:        ..11 .... = Definite or exception chain response
SNA:        .... 0... = 2-phase commit not supported
SNA:        .... ..0. = Compression will not be used
SNA:        .... ...0 = Will not send end bracket
SNA:  Secondary flags = B0
SNA:        1... .... = Multiple RU chains allowed
SNA:        .0.. .... = Immediate request mode
SNA:        ..11 .... = Definite or exception chain response
SNA:        .... 0... = 2-phase commit not supported
SNA:        .... ..0. = Compression will not be used
SNA:        .... ...0 = Will not send end bracket
SNA:  Common flags #1 = D1
SNA:        1... .... = Receipt of segments not supported
SNA:        .1.. .... = FM headers allowed
SNA:        ..0. .... = Brackets are not used or reset states are INB
SNA:        ...1 .... = Conditional bracket termination will be used
SNA:        .... 0... = Alternate code set will not be used
SNA:        .... .0.. = Sequence numbers not available for sync points
SNA:        .... ..0. = BIS not sent
SNA:        .... ...1 = BIND can be queued
SNA:  Common flags #2 = B1
SNA:        10.. .... = Half-duplex flip-flop
SNA:        ..1. .... = Symmetric responsibility for recovery
SNA:        ...1 .... = Primary is contention winner
SNA:        .... 00.. = Process alternate code as ASCII-7
SNA:        .... ..0. = Control vectors are not included after the SLU
                        name
SNA:        .... ...1 = HDX-FF reset state is SEND for the primary
SNA:  Secondary send    window size = 1 (One-stage pacing)
SNA:  Secondary receive window size = 0 (Adaptive pacing not
                                         supported)
```

```
SNA:  Maximum RU size sent by secondary LU = 480
SNA:  Maximum RU size sent by   primary LU = 480
SNA:  Primary send    window size = 0 (Two-stage pacing)
SNA:  Primary receive window size = 1
SNA:  LU type = 6
SNA:  LU level = 2
SNA:  PS flags #1 = 10
SNA:    ...1 .... = Access security info field will be accepted
SNA:    .... ..0. = Already verified indicator will not be accepted
SNA:  PS flags #2 = 23
SNA:    .01. .... = Synchronization confirm supported
SNA:    .... 00.. = Operator controlled session reinitiation
SNA:    .... ..1. = Parallel session supported
SNA:    .... ...1 = Change number of sessions GDS variable flow
                    supported
SNA:  PS Flags #3 = 0X
SNA:    .0.. .... = Contention-winner will not deactivate session
SNA:  Cryptography options = 0X
SNA:             00.. .... = Private cryptography not supported
SNA:             ..00 .... = Session-level cryptography not supported
SNA:             .... 0000 = Length of cryptography options = 0
SNA:  Primary LU name = "....K.....@@@"
SNA:  Length of user data = 29
SNA:  User data key = 0 (Structured subfields follow)
SNA:  Structured data subfield number = 2 (Mode name)
SNA:   Mode name = "......."
SNA:  Structured data subfield number = 3 (Session instance
                                           identifier)
SNA:   Format = 0
SNA:   Session instance identifier = 07
SNA:  Structured data subfield number = 4 (Network-qualified PLU
                                           network name)
SNA:   Network-qualified PLU network name = "....K.....@@@"
SNA:  Length of user request correlation field = 0
SNA:  Length of secondary LU name = 8
SNA:  Secondary LU name = "......@@"
SNA:

ADDR  HEX                                                ASCII
0000  08 00 5A 1A 60 BE 02 00  00 00 00 40 00 5E 04 04  ..Z.`......@.^..
0010  44 B8 2F 00 01 01 00 00  6B 80 00 31 00 13 07 B0  D./.....k..1....
0020  B0 D1 B1 01 00 F5 F5 80  01 06 02 00 00 00 00 00  ................
0030  00 00 10 23 00 00 0D C1  D7 D7 D5 4B D7 C3 D4 C7  ...#.......K....
0040  F1 40 40 40 1D 00 08 02  D8 D7 C3 E2 E4 D7 D7 03  .@@@............
0050  03 00 07 0E 04 C1 D7 D7  D5 4B D7 C3 D4 C7 F1 40  .........K.....@
0060  40 40 00 08 D7 D6 D3 C9  C1 E2 40 40              @@........@@
```

B.2.2 IBM Netbios

Il pacchetto seguente è un pacchetto SMB (Server Message Block) generato probabilmente da un personal computer, imbustato nel protocollo Netbios IBM (Netbeui), imbustato in un pacchetto LLC information (LLC connesso o di tipo 2), imbustato in un pacchetto 802.3 generato da un elaboratore con indirizzo MAC 02-60-8C-74-11-78 (OUI = 02-60-8C, cioè 3Com). Il pacchetto SMB richiede l'apertura di un file remoto. La codifica del SAP LLC user defined del Netbios IBM è F0. Il pacchetto LLC ha numero di sequenza 109 e porta un NAK per piggybacking del frame numero 29.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 1 arrived at  09:18:37.3543; frame size is 143 (008F hex)
      bytes.
DLC:  Destination = Station 3Com  676974
DLC:  Source      = Station 3Com  741178
DLC:  802.3 length = 129
DLC:
LLC:  ----- LLC Header -----
LLC:
LLC:  DSAP = F0, SSAP = F0, Command, I frame, N(R) = 29, N(S) = 109
LLC:
NETB: ----- NETBIOS Data Only Last -----
NETB:
NETB: Header length = 14, Data length = 111
NETB: Delimiter = EFFF (NETBIOS)
NETB: Command = 16
NETB: Flags = X0
NETB: .... 0... = No Acknowledge_Included
NETB: .... .0.. = No Ack_with_data_allowed
NETB: .... ..0. = No NO.ACK indicator
NETB: Re-synch indicator = 0
NETB: Response correlator = 166B
NETB: Remote session number = 25
NETB: Local session number = 1
NETB:
SMB:  ----- SMB Open & more Command -----
SMB:
SMB:  Function = 2D (Open & more)
SMB:  Tree id      (TID) = 0818
SMB:  Process id   (PID) = 0005
SMB:  Multiplex id (MID) = 0794
SMB:  File pathname = "\3COM\MSBENCH\SYNC.CMD"
SMB:  Additional information = 0001
SMB:    .... ....  .... .0.. = Notify about another file open
SMB:    .... ....  .... ..0. = Do not lock file
SMB:    .... ....  .... ...1 = Return additional information
```

```
SMB:  File open mode = 0040
SMB:   .0.. ....  .... .... = Not write through mode
SMB:   .... ....  .100 .... = Shared open (allow others to read/write/
                                           execute)
SMB:   .... ....  .... .000 = Open file for reading
SMB:  Search attributes = 0016
SMB:   .... ....  ..0. .... = File(s) not changed since last archive
SMB:   .... ....  ...1 .... = Directory file(s)
SMB:   .... ....  .... 0... = No volume label info
SMB:   .... ....  .... .1.. = System file(s)
SMB:   .... ....  .... ..1. = Hidden file(s)
SMB:   .... ....  .... ...0 = No read only file(s)
SMB:  Attribute flags = 0020
SMB:   .... ....  ..1. .... = File(s) changed and not archived
SMB:   .... ....  ...0 .... = No directory file(s)
SMB:   .... ....  .... 0... = No volume label info
SMB:   .... ....  .... .0.. = No system file(s)
SMB:   .... ....  .... ..0. = No hidden file(s)
SMB:   .... ....  .... ...0 = No read only file(s)
SMB:  Creation date: none supplied
SMB:  Open function = 0001
SMB:   .... ....  ...0 .... = If file doesn't exist, fail
SMB:   .... ....  .... ..01 = If file exists, open it
SMB:  Bytes to reserve on create or truncate = 0
SMB:  Time to wait for completion: default
SMB:
SMB:  ----- SMB Read & more Command -----
SMB:
SMB:  Function = 2E (Read & more)
SMB:  File handle = 0000
SMB:  Offset in file = 0
SMB:  Maximum read count = 4096 bytes
SMB:  Minimum read count = 0 bytes
SMB:  Time to wait for completion: no delay
SMB:  Bytes remaining to read = 0
SMB:
SMB:  ----- End of SMB chain -----
SMB:

ADDR  HEX                                             ASCII
0000  02 60 8C 67 69 74 02 60  8C 74 11 78 00 81 F0 F0  .`.git.`.t.x....
0010  DA 3A 0E 00 FF EF 16 00  00 00 00 00 6B 16 19 01  .:..........k...
0020  FF 53 4D 42 2D 00 00 00  00 08 00 00 00 00 00 00  .SMB-...........
0030  00 00 00 00 00 00 00 00  18 08 05 00 00 00 94 07  ................
0040  0F 2E 00 58 00 01 00 40  00 16 00 20 00 00 00 00  ...X...@... ....
0050  00 01 00 00 00 00 00 FE  FF FF FF 00 00 00 00 17  ................
0060  00 5C 33 43 4F 4D 5C 4D  53 42 45 4E 43 48 5C 53  .\3COM\MSBENCH\S
0070  59 4E 43 2E 43 4D 44 00  0A FF 00 00 00 00 00 00  YNC.CMD.........
0080  00 00 00 00 10 00 00 00  00 00 00 00 00 00 00 00  ................
```

B.2.3 IBM Network Management

Il pacchetto seguente è un pacchetto di network management (LLC-DSAP = F4). Si tratta di un unnumbered frame cui corrisponde un campo LLC control di un byte contenente il valore 03. Il pacchetto è trasmesso in multicast a livello MAC all'indirizzo 03-00-00-00-00-10.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 45 arrived at  00:03:39.1305; frame size is 109 (006D hex)
      bytes.
DLC:  Destination = Multicast 030000000010
DLC:  Source      = Station 02000000805E
DLC:  802.3 length = 95
DLC:
LLC:  ----- LLC Header -----
LLC:
LLC:  DSAP = F4, SSAP = E4, Command, Unnumbered frame: UI
LLC:
IBMNM: ----- IBM Network Management -----
IBMNM:
IBMNM: Unknown major vector code point = 9006
IBMNM:     Unknown complex subvector code point = 8001
IBMNM:         Ring number = 000
IBMNM:         (Warning: Next vector should be length 6 but is 10)
IBMNM:         Number of alternate LAN Managers = 49152
IBMNM:         (Warning: Next vector should be length 6 but is 8)
IBMNM:         Ring status = 0000 (Operational)
IBMNM:         MAC address = IBM   000000
IBMNM:     Port Information
IBMNM:         (Warning: Next vector should be length 12 but is 6)
IBMNM:         Password key = ""
IBMNM:         Unknown atomic vector type C00C
IBMNM:         Status code = 0000 (Control lost)
IBMNM:         Reason code = 0000 (Normal termination)
IBMNM:         Unknown atomic vector type C00F
IBMNM:         (Warning: Next vector should be length 14 but is 8)
IBMNM:         Microcode level = ""
IBMNM:         (Warning: Next vector should be length 10 but is 8)
IBMNM:         Status = 00000010
IBMNM:
IBMNM: [Normal end of "IBM Network Management".]
IBMNM:

ADDR  HEX                                             ASCII
0000  03 00 00 00 00 10 02 00  00 00 80 5E 00 5F F4 E4  ...........^._..
0010  03 00 5C 90 06 00 26 80  01 00 06 40 05 00 00 00  ..\...&....@....
0020  0A C0 04 C0 00 00 00 00  00 00 08 C0 05 00 00 00  ................
```

```
0030  00 00 0A 40 02 10 00 5A  00 00 00 00 32 80 03 00  ...@...Z....2...
0040  06 C0 0B 00 00 00 06 C0  0C 00 00 00 06 C0 0D 00  ................
0050  00 00 06 C0 0E 00 00 00  06 C0 0F 00 00 00 08 C0  ................
0060  10 00 00 00 01 00 08 C0  11 00 00 00 10          ............
```

B.3 TCP/IP

I pacchetti riportati nei seguenti sottoparagrafi appartengono tutti all'architettura di rete TCP/IP che comprende non solo i protocolli TCP e IP, ma anche molti altri quali UDP, ARP, BOOTP, ecc., e che più in generale andrebbe definita "internet technology".

B.3.1 Telnet

Il seguente pacchetto è generato dall'applicazione telnet che fornisce la funzionalità di terminale virtuale di un host remoto. Il pacchetto telnet è imbustato nel protocollo TCP, imbustato nel protocollo IP, imbustato in un pacchetto MAC di tipo Ethernet. Infatti i due byte che seguono i MAC address contengono il valore esadecimale 0800 che è maggiore di 1500 e quindi indica un pacchetto Ethernet ed assume il significato di protocol type (800 è il protocol type dell'IP). Il pacchetto ha due indirizzi MAC di tipo singolo, uno corrispondente ad una scheda IBM (OUI = 08-00-5A) e l'altra ad una scheda su cui opera anche il protocollo DECnet fase IV (OUI = AA-00-04). Che il pacchetto provenga da un'applicazione telnet risulta evidente poiché la source port nell'header TCP è 23, che è quella associata al telnet.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 2 arrived at  16:55:17.7676; frame size is 60 (003C hex)
      bytes.
DLC:  Destination = Station DECnet009A7D
DLC:  Source      = Station IBM   1A60BE
DLC:  Ethertype  = 0800 (IP)
DLC:
IP:   ----- IP Header -----
IP:
IP:   Version = 4, header length = 20 bytes
IP:   Type of service = 00
IP:         000. .... = routine
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 44 bytes
```

```
IP:   Identification = 22755
IP:   Flags = 0X
IP:   .0.. .... = may fragment
IP:   ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 60 seconds/hops
IP:   Protocol = 6 (TCP)
IP:   Header checksum = 1853 (correct)
IP:   Source address = [130.192.4.18]
IP:   Destination address = [130.192.4.4]
IP:   No options
IP:
TCP:  ----- TCP header -----
TCP:
TCP:  Source port = 1044
TCP:  Destination port = 23 (Telnet)
TCP:  Initial sequence number = 866657824
TCP:  Acknowledgment number = 1449600001
TCP:  Data offset = 24 bytes
TCP:  Flags = 12
TCP:  ..0. .... = (No urgent pointer)
TCP:  ...1 .... = Acknowledgment
TCP:  .... 0... = (No push)
TCP:  .... .0.. = (No reset)
TCP:  .... ..1. = SYN
TCP:  .... ...0 = (No FIN)
TCP:  Window = 16384
TCP:  Checksum = 722D (correct)
TCP:
TCP:  Options follow
TCP:  Maximum segment size = 1451
TCP:

ADDR  HEX                                                ASCII
0000  AA 00 04 00 9A 7D 08 00  5A 1A 60 BE 08 00 45 00  .....}..Z.`...E.
0010  00 2C 58 E3 00 00 3C 06  18 53 82 C0 04 12 82 C0  .,X...<..S......
0020  04 04 04 14 00 17 33 A8  26 20 56 67 24 01 60 12  ......3.& Vg$.`.
0030  40 00 72 2D 00 00 02 04  05 AB 00 00             @.r-........
```

B.3.2 Bootp

Bootp è un protocollo per il bootstrap di stazioni diskless. La richiesta di downloading del sistema operativo viene inviata in broadcast (MAC-DSAP = FF-FF-FF-FF-FF-FF). Il pacchetto bootp viene imbustato in un pacchetto UDP, che viene imbustato in un pacchetto IP, che viene imbustato in un pacchetto Ethernet. Nell'header

IP è indicato che il protocollo sovrastante è UDP (Protocol = 17), mentre nell'header UDP è indicato che si tratta dell'applicativo Bootp (Source port = 68). La stazione che ha inviato il pacchetto monta una scheda 802.3 Digital (OUI = 08-00-2B).

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 6 arrived at  00:48:05.8680; frame size is 342 (0156 hex)
      bytes.
DLC:  Destination = BROADCAST FFFFFFFFFFFF, Broadcast Ethernet
DLC:  Source      = Station DEC   28C3A5
DLC:  Ethertype  = 0800 (IP)
DLC:
IP:   ----- IP Header -----
IP:
IP:   Version = 4, header length = 20 bytes
IP:   Type of service = 00
IP:         000. .... = routine
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 328 bytes
IP:   Identification = 17069
IP:   Flags = 0X
IP:   .0.. .... = may fragment
IP:   ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 30 seconds/hops
IP:   Protocol = 17 (UDP)
IP:   Header checksum = 58F9 (correct)
IP:   Source address = [0.0.0.0]
IP:   Destination address = [255.255.255.255]
IP:   No options
IP:
UDP:  ----- UDP Header -----
UDP:
UDP:  Source port = 68 (Bootp client)
UDP:  Destination port = 67
UDP:  Length = 308
UDP:  No checksum
UDP:
BOOTP:  ----- BOOTP Header -----
BOOTP:
BOOTP:  Boot record type        = 1 (Request)
BOOTP:  Hardware address type   = 1 10Mb Ethernet
BOOTP:  Hardware address length = 6 bytes
BOOTP:
BOOTP:  Hops = 0
BOOTP:  Transaction id = 26423391
```

```
BOOTP:  Elapsed boot time = -21640 seconds
BOOTP:
BOOTP:  Client self-assigned IP address   = [0.0.0.0] (Unknown)
BOOTP:  Client hardware address           = DEC   28C3A5
BOOTP:
BOOTP:  Host name      = ""
BOOTP:  Boot file name = ""
BOOTP:
BOOTP:  Vendor Information tag = 63825363
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
```

```
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:  Pad byte
BOOTP:
```

```
ADDR  HEX                                                ASCII
0000  FF FF FF FF FF FF 08 00  2B 28 C3 A5 08 00 45 00  ........+(....E.
0010  01 48 42 AD 00 00 1E 11  58 F9 00 00 00 00 FF FF  .HB.....X.......
0020  FF FF 00 44 00 43 01 34  00 00 01 01 06 00 26 42  ...D.C.4......&B
0030  33 91 AB 78 00 00 00 00  00 00 00 00 00 00 00 00  3..x............
0040  00 00 00 00 00 00 08 00  2B 28 C3 A5 00 00 00 00  ........+(......
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0110  00 00 00 00 00 00 63 82  53 63 00 00 00 00 00 00  ......c.Sc......
0120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0150  00 00 00 00 00 00                                 ......
```

B.3.3 ARP/RARP

Il protocollo ARP/RARP serve per mantenere una tabella di corrispondenza tra gli indirizzi di livello 3 IP e gli indirizzi di livello 2 MAC. In questo caso la stazione con MAC-DSAP 00-00-0C-00-4D-10 e IP address 130.192.2.17 (un router Cisco) vuole scoprire l'indirizzo MAC della stazione che ha indirizzo IP 130.192.2.46 e a tal fine nel pacchetto ARP/RARP specifica un target hardware address = 00-00-00-00-00-00. La richiesta è inviata con un pacchetto Ethernet in broadcast. Il protocol type di ARP/RARP è 806.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 164 arrived at  00:48:09.9282; frame size is 60 (003C hex)
      bytes.
DLC:  Destination = BROADCAST FFFFFFFFFFFF, Broadcast Ethernet
DLC:  Source      = Station Cisco 004D10, GARR-gw
DLC:  Ethertype  = 0806 (ARP)
DLC:
ARP:  ----- ARP/RARP frame -----
ARP:
ARP:  Hardware type = 1 (10Mb Ethernet)
ARP:  Protocol type = 0800 (IP)
ARP:  Length of hardware address = 6 bytes
ARP:  Length of protocol address = 4 bytes
ARP:  Opcode 1 (ARP request)
ARP:  Sender's hardware address = Cisco 004D10, GARR-gw
ARP:  Sender's protocol address = [130.192.2.17]
ARP:  Target hardware address = 000000000000
ARP:  Target protocol address = [130.192.2.46]
ARP:

ADDR  HEX                                                ASCII
0000  FF FF FF FF FF FF 00 00  0C 00 4D 10 08 06 00 01  ..........M.....
0010  08 00 06 04 00 01 00 00  0C 00 4D 10 82 C0 02 11  ..........M.....
0020  00 00 00 00 00 00 82 C0  02 2E 4A 9A E6 68 03 FD  ..........J..h..
0030  00 00 00 00 00 00 05 63  73 65 6C 74              .......cselt
```

B.3.4 RWHO

Rwho è un applicativo che appartiene al gruppo Runix, cui appartengono anche rcp, rlogin, ecc. Rwho invia in broadcast alcune informazioni relative ad un elaboratore, quali gli utenti collegati, la percentuale di utilizzo, il tempo intercorso dal bootstrap, ecc. Il pacchetto Rwho è imbustato in UDP, che è imbustato in IP, che è imbustato in Ethernet. La porta UDP di Rwho è 513.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 223 arrived at  00:48:11.3466; frame size is 102
      (0066 hex) bytes.
DLC:  Destination = BROADCAST FFFFFFFFFFFF, Broadcast Ethernet
DLC:  Source      = Station H-P   1375F0
DLC:  Ethertype  = 0800 (IP)
DLC:
IP:   ----- IP Header -----
IP:
IP:   Version = 4, header length = 20 bytes
IP:   Type of service = 00
IP:         000. .... = routine
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 88 bytes
IP:   Identification = 19497
IP:   Flags = 0X
IP:   .0.. .... = may fragment
IP:   ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 30 seconds/hops
IP:   Protocol = 17 (UDP)
IP:   Header checksum = 458C (correct)
IP:   Source address = [130.192.2.97]
IP:   Destination address = [130.192.2.255]
IP:   No options
IP:
UDP:  ----- UDP Header -----
UDP:
UDP:  Source port = 513 (Remote who)
UDP:  Destination port = 513
UDP:  Length = 68
UDP:  Checksum = C57C (correct)
UDP:
RUnix: ----- Remote who frame -----
RUnix:
RUnix: Version = 1
RUnix: Type = 1
RUnix: Send time = 30-May-94 22:41:30 GMT
RUnix: Receive time = 0
RUnix: Host = "meucci"
RUnix: Load average = 0.00 (5-minute), 0.00 (10-minute),
       0.00 (15-minute)
RUnix: Boot time = 19-Apr-94 18:02:03 GMT
RUnix: Nobody logged on
RUnix:
RUnix: [Normal end of "Remote who frame".]
RUnix:
```

```
ADDR  HEX                                                ASCII
0000  FF FF FF FF FF FF 08 00  09 13 75 F0 08 00 45 00  ..........u...E.
0010  00 58 4C 29 00 00 1E 11  45 8C 82 C0 02 61 82 C0  .XL)....E....a..
0020  02 FF 02 01 02 01 00 44  C5 7C 01 01 00 00 2D EA  .......D.|....-.
0030  6B 9A 00 00 00 00 6D 65  75 63 63 69 00 00 00 00  k.....meucci....
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0060  00 00 2D B4 1C 9B                                  ..-...
```

B.3.5 NFS

NFS è il Network File System, un file system distribuito su rete e concepito esplicitamente per il mondo internet. Il pacchetto NFS è imbustato in RPC (Remote Procedural Call), che è imbustato in UDP e via di seguito. RPC è la porta 1021 di UPD e NFS è il Program = 100003 di RPC. Tali numeri di porta non sono previsti dallo standard RFC 1340, ma sono generati dinamicamente dall'applicativo "portmap".

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 154 arrived at  00:48:09.8085; frame size is 278
      (0116 hex) bytes.
DLC:  Destination = Station Cisco 004D10, GARR-gw
DLC:  Source      = Station DEC   37E61F
DLC:  Ethertype  = 0800 (IP)
DLC:
IP:   ----- IP Header -----
IP:
IP:   Version = 4, header length = 20 bytes
IP:   Type of service = 00
IP:         000. .... = routine
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 264 bytes
IP:   Identification = 44847
IP:   Flags = 0X
IP:   .0.. .... = may fragment
IP:   ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 30 seconds/hops
IP:   Protocol = 17 (UDP)
IP:   Header checksum = E027 (correct)
IP:   Source address = [130.192.5.4]
IP:   Destination address = [130.192.2.10]
IP:   No options
IP:
```

```
UDP:  ----- UDP Header -----
UDP:
UDP:  Source port = 1021 (Sun RPC)
UDP:  Destination port = 2049
UDP:  Length = 244
UDP:  Checksum = 85A2 (correct)
UDP:
RPC:  ----- SUN RPC header -----
RPC:
RPC:  Transaction id = 2142883117
RPC:  Type = 0 (Call)
RPC:  RPC version = 2
RPC:  Program = 100003 (NFS), version = 2
RPC:  Procedure = 8 (Write to file)
RPC:  Credentials: authorization flavor = 1 (Unix)
RPC:   len = 40, stamp = 770312100
RPC:   machine = polpl5.polito.it
RPC:   uid = 2029, gid = 2000
RPC:   1 other group id(s):
RPC:    gid 2000
RPC:  Verifier: authorization flavor = 0 (Null)
RPC:  [Verifier: 0 byte(s) of authorization data]
RPC:
RPC:  [Normal end of "SUN RPC header".]
RPC:
NFS:  ----- SUN NFS -----
NFS:
NFS:  Proc = 8 (Write to file)
NFS:  File handle = 0A1500001A1000008AB3070802000000
NFS:                B8B2067B00000000000000000000000000
NFS:  Offset = 131072
NFS:  [108 byte(s) of data]
NFS:
NFS:  [Normal end of "SUN NFS".]
NFS:

ADDR  HEX                                             ASCII
0000  00 00 0C 00 4D 10 08 00  2B 37 E6 1F 08 00 45 00  ....M...+7....E.
0010  01 08 AF 2F 00 00 1E 11  E0 27 82 C0 05 04 82 C0  .../.....'......
0020  02 0A 03 FD 08 01 00 F4  85 A2 7F B9 CD 2D 00 00  .............-..
0030  00 00 00 00 00 02 00 01  86 A3 00 00 00 02 00 00  ................
0040  00 08 00 00 00 01 00 00  00 28 2D EA 07 A4 00 00  .........(-.....
0050  00 10 70 6F 6C 70 6C 35  2E 70 6F 6C 69 74 6F 2E  ..polpl5.polito.
0060  69 74 00 00 07 ED 00 00  07 D0 00 00 00 01 00 00  it..............
0070  07 D0 00 00 00 00 00 00  00 00 0A 15 00 00 1A 10  ................
0080  00 00 8A B3 07 08 02 00  00 00 B8 B2 06 7B 00 00  .............{..
0090  00 00 00 00 00 00 00 00  00 00 00 02 00 00 00 02  ................
00A0  00 00 00 00 00 6C 00 00  00 6C 20 20 20 20 20 20  .....l...l
00B0  20 20 32 30 34 39 20 44  27 41 47 4F 53 54 49 4E    2049 D'AGOSTIN
```

```
00C0  4F 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20  O
00D0  20 20 20 20 20 0A 20 20  63 70 75 20 3A 20 20 35       .  cpu :  5
00E0  2E 36 36 20 73 65 63 2E  20 0A 20 20 20 20 20 20  .66 sec. .
00F0  20 20 32 30 35 30 20 4D  4F 54 54 41 20 20 20 20    2050 MOTTA
0100  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0110  20 20 20 20 20 0A                                       .
```

B.3.6 TFTP

Il TFTP è il Trivial File Transfer Protocol utilizzato per effettuare un file transfer molto semplici su internet. TFTP è associato alla porta 69 di UDP che è imbustato in IP e così via. In questo caso il TFTP chiede di leggere il file \config.sys sul calcolatore con indirizzo IP 128.1.0.1 e indirizzo MAC 00-00-C0-E5-8C-11. Il calcolatore monta una scheda di rete locale Western Digital (OUI = 00-00-C0).

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 3 arrived at  13:41:17.9026; frame size is 75 (004B hex)
      bytes.
DLC:  This frame is dated 17 day(s) after capture started.
DLC:  Destination = Station WstDigE58C11
DLC:  Source      = Station WstDig488C11
DLC:  Ethertype  = 0800 (IP)
DLC:
IP:   ----- IP Header -----
IP:
IP:   Version = 4, header length = 20 bytes
IP:   Type of service = 00
IP:         000. .... = routine
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 61 bytes
IP:   Identification = 1
IP:   Flags = 0X
IP:   .0.. .... = may fragment
IP:   ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 255 seconds/hops
IP:   Protocol = 17 (UDP)
IP:   Header checksum = BBA9 (correct)
IP:   Source address = [128.1.0.2]
IP:   Destination address = [128.1.0.1]
IP:   No options
IP:
```

```
UDP:  ----- UDP Header -----
UDP:
UDP:  Source port = 1004 (TFTP)
UDP:  Destination port = 69
UDP:  Length = 41
UDP:  Checksum = BBED (correct)
UDP:
TFTP:  ----- Trivial file transfer -----
TFTP:
TFTP:  Opcode = 1 (Read request)
TFTP:  File name = "\config.sys"
TFTP:  Mode = "netascii"
TFTP:
TFTP:  *** 10 byte(s) of additional data present ***
TFTP:
TFTP:  [Abnormal end of "Trivial file transfer".]
TFTP:

ADDR  HEX                                                ASCII
0000  00 00 C0 E5 8C 11 00 00  C0 48 8C 11 08 00 45 00 .........H....E.
0010  00 3D 00 01 00 00 FF 11  BB A9 80 01 00 02 80 01 .=..............
0020  00 01 03 EC 00 45 00 29  BB ED 00 01 5C 63 6F 6E .....E.)....\con
0030  66 69 67 2E 73 79 73 00  6E 65 74 61 73 63 69 69 fig.sys.netascii
0040  00 00 00 00 00 00 00 00  00 00 00               ...........
```

B.3.7 DNS

Il DNS è il Domain Name Service, cioè quell'applicativo di rete che serve per tradurre i nomi negli indirizzi IP e viceversa. DNS si appoggia sulla porta 53 di UDP, UDP viene imbustato in IP, ecc. La query DNS vuole scoprire l'indirizzo dell'host ercole.polito.it.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 728 arrived at  00:48:24.2087; frame size is 76 (004C hex)
bytes.
DLC:  Destination = Station DECnet00E97D, ERCOLE
DLC:  Source      = Station DEC   181C22
DLC:  Ethertype  = 0800 (IP)
DLC:
IP:   ----- IP Header -----
IP:
IP:   Version = 4, header length = 20 bytes
IP:   Type of service = 00
IP:         000. .... = routine
IP:         ...0 .... = normal delay
```

```
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 62 bytes
IP:   Identification = 15103
IP:   Flags = 0X
IP:   .0.. .... = may fragment
IP:   ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 30 seconds/hops
IP:   Protocol = 17 (UDP)
IP:   Header checksum = 5623 (correct)
IP:   Source address = [130.192.3.12]
IP:   Destination address = [130.192.3.1]
IP:   No options
IP:
UDP:  ----- UDP Header -----
UDP:
UDP:  Source port = 2076 (Domain)
UDP:  Destination port = 53
UDP:  Length = 42
UDP:  Checksum = B149 (correct)
UDP:
DNS:  ----- Internet Domain Name Service header -----
DNS:
DNS:  ID = 9346
DNS:  Flags = 01
DNS:  0... .... = Command
DNS:  .000 0... = Query
DNS:  .... ..0. = Not truncated
DNS:  .... ...1 = Recursion desired
DNS:  Flags = 0X
DNS:  ...0 .... = Unicast packet
DNS:  Question count = 1, Answer count = 0
DNS:  Authority count = 0, Additional record count = 0
DNS:
DNS:  Question section:
DNS:      Name = ercole.polito.it
DNS:      Type = Host address (A,1)
DNS:      Class = Internet (IN,1)
DNS:
DNS:  [Normal end of "Internet Domain Name Service header".]
DNS:

ADDR  HEX                                               ASCII
0000  AA 00 04 00 E9 7D 08 00  2B 18 1C 22 08 00 45 00  .....}..+.."..E.
0010  00 3E 3A FF 00 00 1E 11  56 23 82 C0 03 0C 82 C0  .>:.....V#......
0020  03 01 08 1C 00 35 00 2A  B1 49 24 82 01 00 00 01  .....5.*.I$.....
0030  00 00 00 00 00 00 06 65  72 63 6F 6C 65 06 70 6F  .......ercole.po
0040  6C 69 74 6F 02 69 74 00  00 01 00 01              lito.it.....
```

B.3.8 X Windows

X Windows è indubbiamente uno degli applicativi più interessanti e moderni che possono essere trasportati su una rete internet. Il pacchetto X Windows in oggetto chiede di visualizzare la scritta "New mail on node POL88B from IN%"VANNOZZI@NIS.GARR.IT" "Daniele Vannozzi"" su una finestra X, collocata sull'host con indirizzo IP 130.192.5.41 e indirizzo MAC 08-00-2B-39-02-21. La richiesta è associata alla porta 6000 di TCP ed è generata dall'host con nome POL88B, indirizzo IP 130.192.2.16 e indirizzo MAC AA-00-04-00-92-7D.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 860 arrived at  00:48:27.3165; frame size is 274
      (0112 hex) bytes.
DLC:  Destination = Station DEC   390221
DLC:  Source      = Station DECnet00927D, POL88B
DLC:  Ethertype  = 0800 (IP)
DLC:
IP:   ----- IP Header -----
IP:
IP:   Version = 4, header length = 20 bytes
IP:   Type of service = 00
IP:         000. .... = routine
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 260 bytes
IP:   Identification = 36610
IP:   Flags = 0X
IP:   .0.. .... = may fragment
IP:   ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 60 seconds/hops
IP:   Protocol = 6 (TCP)
IP:   Header checksum = E238 (correct)
IP:   Source address = [130.192.2.16]
IP:   Destination address = [130.192.5.41]
IP:   No options
IP:
TCP:  ----- TCP header -----
TCP:
TCP:  Source port = 4005
TCP:  Destination port = 6000 (X Windows)
TCP:  Sequence number = 941492665
TCP:  Acknowledgment number = 84081
TCP:  Data offset = 20 bytes
TCP:  Flags = 18
```

```
TCP:  ..0. .... = (No urgent pointer)
TCP:  ...1 .... = Acknowledgment
TCP:  .... 1... = Push
TCP:  .... .0.. = (No reset)
TCP:  .... ..0. = (No SYN)
TCP:  .... ...0 = (No FIN)
TCP:  Window = 6144
TCP:  Checksum = 9800 (correct)
TCP:  No TCP options
TCP:  [220 byte(s) of data]
TCP:
XWIN: ----- X Windows -----
XWIN:
XWIN: Request opcode = 70 (Poly Fill Rectangle)
XWIN: Drawable = 00300015, Graphics context = 0030001A
XWIN: X = 70, Y = 464, Width = 11, Height = 20
XWIN:
XWIN: Request opcode = 56 (Change GC)
XWIN: Graphics context = 00300016
XWIN: Value mask = 00010000
XWIN: Graphics exposures = 1 (True)
XWIN:
XWIN: Request opcode = 62 (Copy Area)
XWIN: Source drawable = 00300015
XWIN: Destination drawable = 00300015
XWIN: Graphics context = 00300016
XWIN: Source X = 4, Y = 24
XWIN: Destination X = 4, Y = 4
XWIN: Width = 880, Height = 460
XWIN:
XWIN: Request opcode = 61 (Clear Area)
XWIN: Exposures = 0 (False)
XWIN: Window = 00300015
XWIN: X = 4, Y = 464, Width = 880, Height = 20
XWIN:
XWIN: Request opcode = 104 (Bell)
XWIN: Percent = 0
XWIN:
XWIN: Request opcode = 76 (Image Text8)
XWIN: Drawable = 00300015, Graphics context = 00300027
XWIN: X = 4, Y = 479
XWIN: String = "New mail on node POL88B from IN%"VANNOZZI@NIS.GARR.IT"
      "Daniele Vannozzi""
XWIN:
XWIN: Request opcode = 62 (Copy Area)
XWIN: Source drawable = 00300015
XWIN: Destination drawable = 00300015
XWIN: Graphics context = 00300016
XWIN: Source X = 4, Y = 24
```

```
XWIN: Destination X = 4, Y = 4
XWIN: Width = 880, Height = 460
XWIN:
XWIN: Request opcode = 61 (Clear Area)
XWIN: Exposures = 0 (False)
XWIN: Window = 00300015
XWIN: X = 4, Y = 464, Width = 880, Height = 20
XWIN:

ADDR  HEX                                                ASCII
0000  08 00 2B 39 02 21 AA 00  04 00 92 7D 08 00 45 00  ..+9.!.....}..E.
0010  01 04 8F 02 00 00 3C 06  E2 38 82 C0 02 10 82 C0  ......<..8......
0020  05 29 0F A5 17 70 38 1E  09 B9 00 01 48 71 50 18  .)...p8.....HqP.
0030  18 00 98 00 00 00 46 00  05 00 15 00 30 00 1A 00  ......F.....0...
0040  30 00 46 00 D0 01 0B 00  14 00 38 00 04 00 16 00  0.F.......8.....
0050  30 00 00 00 01 00 01 00  00 00 3E 00 07 00 15 00  0.........>.....
0060  30 00 15 00 30 00 16 00  30 00 04 00 18 00 04 00  0...0...0.......
0070  04 00 70 03 CC 01 3D 00  04 00 15 00 30 00 04 00  ..p...=.....0...
0080  D0 01 70 03 14 00 68 00  01 00 4C 4A 17 00 15 00  ..p...h...LJ....
0090  30 00 27 00 30 00 04 00  DF 01 4E 65 77 20 6D 61  0.'.0.....New ma
00A0  69 6C 20 6F 6E 20 6E 6F  64 65 20 50 4F 4C 38 38  il on node POL88
00B0  42 20 66 72 6F 6D 20 49  4E 25 22 56 41 4E 4E 4F  B from IN%"VANNO
00C0  5A 5A 49 40 4E 49 53 2E  47 41 52 52 2E 49 54 22  ZZI@NIS.GARR.IT"
00D0  20 20 22 44 61 6E 69 65  6C 65 20 56 61 6E 6E 6F    "Daniele Vanno
00E0  7A 7A 69 22 30 00 3E 00  07 00 15 00 30 00 15 00  zzi"0.>.....0...
00F0  30 00 16 00 30 00 04 00  18 00 04 00 04 00 70 03  0...0.........p.
0100  CC 01 3D 00 04 00 15 00  30 00 04 00 D0 01 70 03  ..=.....0.....p.
0110  14 00                                              ..
```

B.3.9 RIP

Il RIP è il Routing Information Protocol, un protocollo di routing utilizzato su reti IP di dominio pubblico. Il RIP è associato alla porta 520 di UDP. Il pacchetto UDP è imbustato su IP e così via. Il pacchetto è inviato in broadcast a livello MAC dalla stazione AA-00-04-00-CD-7D che ha nome POLME2 e indirizzo IP 130.192.2.147. Si noti che a livello 3 (IP) il broadcast è limitato alla subnet 2 della net 130.192, come appare evidente dall'IP destination address = [130.192.2.255] (255 è appunto il broadcast).

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 1823 arrived at  00:48:51.0046; frame size is 66
      (0042 hex) bytes.
DLC:  Destination = BROADCAST FFFFFFFFFFFF, Broadcast Ethernet
DLC:  Source      = Station DECnet00CD7D, POLME2
```

```
DLC:  Ethertype  = 0800 (IP)
DLC:
IP:   ----- IP Header -----
IP:
IP:   Version = 4, header length = 20 bytes
IP:   Type of service = 00
IP:         000. .... = routine
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 52 bytes
IP:   Identification = 23830
IP:   Flags = 0X
IP:   .0.. .... = may fragment
IP:   ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 30 seconds/hops
IP:   Protocol = 17 (UDP)
IP:   Header checksum = 3491 (correct)
IP:   Source address = [130.192.2.147]
IP:   Destination address = [130.192.2.255]
IP:   No options
IP:
UDP:  ----- UDP Header -----
UDP:
UDP:  Source port = 520 (Route)
UDP:  Destination port = 520
UDP:  Length = 32
UDP:  Checksum = 69C7 (correct)
UDP:
RIP:  ----- RIP Header -----
RIP:
RIP:  Command = 2 (Response)
RIP:  Version = 1
RIP:  Unused  = 0
RIP:
RIP:  Routing data frame 1
RIP:     Address family identifier = 2 (IP)
RIP:     IP Address = [130.192.2.0]
RIP:     Metric     = 1
RIP:

ADDR  HEX                                                ASCII
0000  FF FF FF FF FF FF AA 00  04 00 CD 7D 08 00 45 00  ..........}..E.
0010  00 34 5D 16 00 00 1E 11  34 91 82 C0 02 93 82 C0  .4].....4.......
0020  02 FF 02 08 02 08 00 20  69 C7 02 01 00 00 00 02  ....... i.......
0030  00 00 82 C0 02 00 00 00  00 00 00 00 00 00 00 00  ................
0040  00 01                                            ..
```

B.3.10 YP

L'applicativo YP (Yellow Pages) è un applicativo proposto da SUN ed aggiuntivo rispetto al DNS per gestire i nomi, gli indirizzi, gli UID e i GID in modo centralizzato, caratteristica questa indispensabile per la sicurezza di applicativi quali NFS. In questo caso il server di YP è quello relativo al dominio CISIP.polito.it e si tratta di una workstation Sony che interroga un server SUN. YP è imbustato in RPC, che è imbustato in UDP, che è imbustato in IP, che è imbustato in Ethernet.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 5279 arrived at  00:50:21.2675; frame size is 118
      (0076 hex) bytes.
DLC:  Destination = Station Sun   11F49F
DLC:  Source      = Station Sony  004832
DLC:  Ethertype  = 0800 (IP)
DLC:
IP:   ----- IP Header -----
IP:
IP:   Version = 4, header length = 20 bytes
IP:   Type of service = 00
IP:         000. .... = routine
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 104 bytes
IP:   Identification = 64122
IP:   Flags = 0X
IP:   .0.. .... = may fragment
IP:   ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 30 seconds/hops
IP:   Protocol = 17 (UDP)
IP:   Header checksum = 94CB (correct)
IP:   Source address = [130.192.5.22], poltcux1
IP:   Destination address = [130.192.2.169]
IP:   No options
IP:
UDP:  ----- UDP Header -----
UDP:
UDP:  Source port = 2376
UDP:  Destination port = 660 (Sun RPC)
UDP:  Length = 84
UDP:  No checksum
UDP:
RPC:  ----- SUN RPC header -----
RPC:
```

```
RPC:  Transaction id = 770527999
RPC:  Type = 0 (Call)
RPC:  RPC version = 2
RPC:  Program = 100004 (Yellow pages), version = 2
RPC:  Procedure = 4 (Get first keyu-value pair in map)
RPC:  Credentials: authorization flavor = 0 (Null)
RPC:  [Credentials: 0 byte(s) of authorization data]
RPC:  Verifier: authorization flavor = 0 (Null)
RPC:  [Verifier: 0 byte(s) of authorization data]
RPC:
RPC:  [Normal end of "SUN RPC header".]
RPC:
YP:   ----- SUN Yellow Pages -----
YP:
YP:   Proc = 4 (Get first keyu-value pair in map)
YP:   Domain = CISIP.polito.it
YP:   Map = group.byname
DLC:  --- Frame too short

ADDR  HEX                                                ASCII
0000  08 00 20 11 F4 9F 08 00  46 00 48 32 08 00 45 00  .. .....F.H2..E.
0010  00 68 FA 7A 00 00 1E 11  94 CB 82 C0 05 16 82 C0  .h.z............
0020  02 A9 09 48 02 94 00 54  00 00 2D ED 52 FF 00 00  ...H...T..-.R...
0030  00 00 00 00 00 02 00 01  86 A4 00 00 00 02 00 00  ................
0040  00 04 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0050  00 00 00 00 00 0F 43 49  53 49 50 2E 70 6F 6C 69  ......CISIP.poli
0060  74 6F 2E 69 74 00 00 00  00 0C 67 72 6F 75 70 2E  to.it.....group.
0070  62 79 6E 61 6D 65                                byname
```

B.3.11 SMB su TCP/IP

I pacchetti SMB possono essere imbustati in vari protocolli. In B.2.2 si è analizzato il caso di SMB imbustato in Netbios IBM; qui SMB viene imbustato in TCP (porta 46586), che a sua volta viene imbustato in IP. Naturalmente, perché due protocolli SMB possano parlarsi è indispensabile che tutti gli imbustamenti siano compatibili (un SMB su Netbios IBM non può dialogare con un SMB su TCP/IP).

In questo esempio si vede per la prima volta il trasporto di IP su 802.3. Si sfrutta il LLC con LLC-SSAP e LLC-DSAP uguali a 06, codifica definita dall'IEEE per il Department of Defense Internet Protocol. Altre possibilità sono il trasporto di IP come pacchetto SNAP (descritto nel capitolo 5 e previsto dal RFC 1042) oppure l'utilizzo dell'imbustamento Ethernet come ad esempio in A.3.10.

```
DLC:  ----- DLC Header -----
DLC:
```

```
DLC:  Frame 3 arrived at  14:30:33.0552; frame size is 92 (005C hex)
      bytes.
DLC:  Destination = Station 3Com  138162
DLC:  Source      = Station 3Com  138372
DLC:  802.3 length = 78
DLC:
LLC:  ----- LLC Header -----
LLC:
LLC:  DSAP = 06, SSAP = 06, Command, Unnumbered frame: UI
LLC:
IP:   ----- IP Header -----
IP:
IP:   Version = 4, header length = 20 bytes
IP:   Type of service = 00
IP:         000. .... = routine
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 75 bytes
IP:   Identification = 0
IP:   Flags = 4X
IP:   .1.. .... = don't fragment
IP:   ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 60 seconds/hops
IP:   Protocol = 6 (TCP)
IP:   Header checksum = 8E2B (correct)
IP:   Source address = [15.6.73.50]
IP:   Destination address = [15.6.73.68]
IP:   No options
IP:
TCP:  ----- TCP header -----
TCP:
TCP:  Source port = 5696
TCP:  Destination port = 46586
TCP:  Sequence number = 346879454
TCP:  Acknowledgment number = 1109177
TCP:  Data offset = 20 bytes
TCP:  Flags = 18
TCP:  ..0. .... = (No urgent pointer)
TCP:  ...1 .... = Acknowledgment
TCP:  .... 1... = Push
TCP:  .... .0.. = (No reset)
TCP:  .... ..0. = (No SYN)
TCP:  .... ...0 = (No FIN)
TCP:  Window = 1424
TCP:  Checksum = 0 (No checksum sent)
TCP:  No TCP options
TCP:  [35 byte(s) of data]
```

```
TCP:
SMB:  ----- SMB Spool Byte Range Response -----
SMB:
SMB:  Function = C1 (Spool Byte Range)
SMB:  Tree id      (TID) = 0021
SMB:  Process id   (PID) = 354A
SMB:  Return code = 0,0 (OK)
SMB:

ADDR  HEX                                                ASCII
0000  02 60 8C 13 81 62 02 60  8C 13 83 72 00 4E 06 06  .`...b.`...r.N..
0010  03 45 00 00 4B 00 00 40  00 3C 06 8E 2B 0F 06 49  .E..K..@.<..+..I
0020  32 0F 06 49 44 16 40 B5  FA 14 AC F5 DE 00 10 EC  2..ID.@.........
0030  B9 50 18 05 90 00 00 00  00 FF 53 4D 42 C1 00 00  .P........SMB...
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0050  00 21 00 4A 35 00 00 00  00 00 00 00              .!.J5.......
```

B.3.12 ISODE

ISODE è un ambiente per sviluppare applicazioni OSI su trasporto TCP/IP e renderne estremamente semplice la portabilità su architetture OSI. Si noti come un pacchetto di trasporto OSI è imbustato in un pacchetto di Development Environment, che è imbustato in un pacchetto TCP, che è imbustato in un pacchetto IP, che è imbustato in un pacchetto Ethernet.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 5 arrived at  09:36:42.0164; frame size is 60 (003C hex)
      bytes.
DLC:  Destination = Station Sun   01DA53
DLC:  Source      = Station Exceln518736
DLC:  Ethertype  = 0800 (IP)
DLC:
IP:   ----- IP Header -----
IP:
IP:   Version = 4, header length = 20 bytes
IP:   Type of service = 00
IP:         000. .... = routine
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 46 bytes
IP:   Identification = 4997
IP:   Flags = 0X
IP:   .0.. .... = may fragment
```

```
IP:   ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 60 seconds/hops
IP:   Protocol = 6 (TCP)
IP:   Header checksum = 59C6 (correct)
IP:   Source address = [192.9.200.170]
IP:   Destination address = [192.9.200.193]
IP:   No options
IP:
TCP:  ----- TCP header -----
TCP:
TCP:  Source port = 1082
TCP:  Destination port = 102 (ISO)
TCP:  Sequence number = 1065666
TCP:  Acknowledgment number = 38786
TCP:  Data offset = 20 bytes
TCP:  Flags = 18
TCP:  ..0. .... = (No urgent pointer)
TCP:  ...1 .... = Acknowledgment
TCP:  .... 1... = Push
TCP:  .... .0.. = (No reset)
TCP:  .... ..0. = (No SYN)
TCP:  .... ...0 = (No FIN)
TCP:  Window = 4096
TCP:  Checksum = 9A5C (correct)
TCP:  No TCP options
TCP:  [6 byte(s) of data]
TCP:
ISO_DE: ----- ISO Development Environment -----
ISO_DE:
ISO_DE: Multi-frame TPDU: frames 5, 6, 7
ISO_DE: Version = 3
ISO_DE: Packet length = 22
ISO_DE:
ISO_TP: ----- ISO Transport Layer -----
ISO_TP:
ISO_TP: Header length = 17
ISO_TP: TPDU type = E (Connection request)
ISO_TP: Destination reference = 0000
ISO_TP:      Source reference = 0096
ISO_TP: Additional options = 01
ISO_TP:          .... 0... = No use of network expedited in class 1
ISO_TP:          .... .0.. = Use explicit AK variant in class 1
ISO_TP:          .... ..0. = Use 16-bit checksum in class 4
ISO_TP:          .... ...1 = Use expedited data transfer
ISO_TP:      Source TSAP: "<8096>"
ISO_TP: Destination TSAP: "<0206>"
ISO_TP:
```

```
ADDR  HEX                                              ASCII
0000  08 00 20 01 DA 53 08 00  14 51 87 36 08 00 45 00 .. ..S...Q.6..E.
0010  00 2E 13 85 00 00 3C 06  59 C6 C0 09 C8 AA C0 09 ......<.Y.......
0020  C8 C1 04 3A 00 66 00 10  42 C2 00 00 97 82 50 18 ...:.f..B.....P.
0030  10 00 9A 5C 00 00 03 00  00 16 11 E0             ...\........
```

B.4 DECNET FASE IV

Gli esempi dei sottoparagrafi seguenti sono relativi all'architettura di rete proprietaria DECnet fase IV. L'evoluzione di DECnet nota con il nome di DECnet fase V è invece totalmente compatibile con OSI e per gli esempi si veda il paragrafo A.6.

B.4.1 DAP

Il DAP è il Data Access Protocol, un protocollo usato per accedere a dati su host remoti. Il DAP è imbustato nel Network Service Protocol (NSP, livello 4), che è imbustato nel DECnet Routing Protocol (DRP, livello 3), che è imbustato in Ethernet (protocol type = 6003). Gli indirizzi di livello 3 dei nodi DECnet mittente e destinatario sono rispettivamente 7.45 e 7.52, cioè appartengono entrambi all'area DECnet numero 7.

A questi due indirizzi di livello 3 corrispondono due MAC address AA-00-04-00-2D-1C e AA-00-04-00-34-1C, che sono calcolati algoritmicamente a partire dagli indirizzi di livello 3 e cioè facendo seguire ad AA-00-04-00 i 16 bit dell'indirizzo di livello 3, con i due byte scambiati. Per un esempio di calcolo si veda A.4.3.

All'atto del bootstrap il protocollo DECnet provvede a sostituire gli indirizzi MAC delle schede con quelli calcolati algoritmicamente a partire dagli indirizzi di livello 3.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 13 arrived at  17:01:07.9740; frame size is 71 (0047 hex)
      bytes.
DLC:  Destination = Station DECnet00341C
DLC:  Source      = Station DECnet002D1C
DLC:  Ethertype  = 6003 (DECNET)
DLC:
DRP:  ----- DECNET Routing Protocol -----
DRP:
DRP:  Data Length = 55,  Optional Padding Length = 1
DRP:  Data Packet Format = 26
DRP:           0... .... = no padding
DRP:           .0.. .... = version
```

```
DRP:           ..1. .... = Intra-Ethernet packet
DRP:           ...0 .... = not return packet
DRP:           .... 0... = do not return to sender
DRP:           .... .110 = Long Data Packet Format
DRP:  Data Packet Type = 6
DRP:  Destination Area     = 00
DRP:  Destination Subarea  = 00
DRP:  Destination ID       = 7.52
DRP:  Source Area          = 00
DRP:  Source Subarea       = 00
DRP:  Source ID            = 7.45
DRP:  Next Level 2 Router  = 00
DRP:  Visit Count          = 0
DRP:  Service Class        = 00
DRP:  Protocol Type        = 00
DRP:
NSP:  ----- Network Services Protocol -----
NSP:
NSP:  Message Identifier = 60
NSP:           0... .... = Non-extensible field
NSP:           .110 .... = Begin-End Data Message
NSP:           .... 00.. = Data Message
NSP:           .... ..00 = always zero
NSP:  Type     = 0  (Data Message)
NSP:  Sub-type = 6  (Begin-End Data Message)
NSP:  Logical Link Destination = 1413
NSP:  Logical Link Source      = 0C39
NSP:  Data Acknowledgment Number
NSP:     Acknowledge Qualifier       = ACK
NSP:     Message Number Acknowledged = 1
NSP:  Data Segment Number = 2  (normal ACK expected)
NSP:   [24 data bytes]
NSP:
DAP:  ----- Data Access Protocol -----
DAP:
DAP:  Code = 3  (Access)
DAP:  Access Function = Directory List
DAP:  Access Options Type:
DAP:   Bit  0: I/O errors are non-fatal
DAP:  File Name Specification = "SYS$MANAGER:*.EXE;*"
DAP:

ADDR  HEX                                             ASCII
0000  AA 00 04 00 34 1C AA 00  04 00 2D 1C 60 03 37 00 ....4.....-.`.7.
0010  81 26 00 00 AA 00 04 00  34 1C 00 00 AA 00 04 00 .&......4.......
0020  2D 1C 00 00 00 00 60 13  14 39 0C 01 80 02 00 03 -.....`..9......
0030  00 06 01 13 53 59 53 24  4D 41 4E 41 47 45 52 3A ....SYS$MANAGER:
0040  2A 2E 45 58 45 3B 2A                            *.EXE;*
```

B.4.2 End System Hello

Il seguente pacchetto è un End System Hello del livello 3 DECnet (DRP) generato da un end system con indirizzo 60.975 per essere riconosciuto da un router ed incluso nelle tabelle di instradamento. Il pacchetto è trasmesso all'indirizzo MAC di multicast del DECnet e cioè AB-00-00-03-00-00.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 96 arrived at  00:48:08.1274; frame size is 60 (003C hex)
      bytes.
DLC:  Destination = Multicast AB0000030000
DLC:  Source      = Station DECnet00CFF3
DLC:  Ethertype  = 6003 (DECNET)
DLC:
DRP:  ----- DECNET Routing Protocol -----
DRP:
DRP:  Data length = 33
DRP:  Control Packet Format = 0D
DRP:              0... .... = no padding
DRP:              .000 .... = reserved
DRP:              .... 110. = Ethernet Endnode Hello Message
DRP:              .... ...1 = Control Packet Format
DRP:  Control Packet Type = 06
DRP:  Version Number  = 02
DRP:  ECO Number      = 00
DRP:  User ECO Number = 00
DRP:  ID of Transmitting Node = 60.975
DRP:       Information = 03
DRP:         0... .... = reserved
DRP:         .0.. .... = not blocking request
DRP:         ..0. .... = multicast traffic accepted
DRP:         ...0 .... = verification ok
DRP:         .... 0... = do not reject
DRP:         .... .0.. = no verification required
DRP:         .... ..11 = endnode
DRP:  Receive Block Size    = 1498
DRP:  Area (reserved)       = 0
DRP:  Verification Seed     = 0000000000000000
DRP:  Neighbor System ID    = 60.75
DRP:  Hello timer (seconds) = 30
DRP:  MPD (reserved)        = 0
DRP:  [1 bytes of Data to test the circuit]
DRP:

ADDR  HEX                                              ASCII
0000  AB 00 00 03 00 00 AA 00  04 00 CF F3 60 03 21 00 ............`.!.
0010  0D 02 00 00 AA 00 04 00  CF F3 03 DA 05 00 00 00 ................
```

```
0020  00 00 00 00 00 00 AA 00  04 00 4B F0 1E 00 00 01  ..........K.....
0030  AA 00 00 00 00 00 00 00  00 00 00 00              ............
```

B.4.3 Router Hello

Questo pacchetto differisce dal precedente in quanto trasmesso da un router per farsi conoscere dagli end node. Il router mittente è il 31.458 (nome POLFIS) come si può capire anche dall'indirizzo di mittente MAC. Infatti 31*1024+458 è uguale a 32202, cioè in esadecimale 7D-CA. Invertendo i due byte si ottiene CA-7D e premettendo l'OUI DECnet AA-00-04 si ottiene un MAC-SSAP aa-00-04-00-CA-7D.

Il pacchetto contiene anche gli indirizzi di livello 3 degli altri router collegati alla stessa LAN e cioè: 31.492, 31.501, 31.402, 31.401 e 31.412.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 139 arrived at  00:48:09.3545; frame size is 78 (004E hex)
      bytes.
DLC:  Destination = Multicast AB0000030000
DLC:  Source      = Station DECnet00CA7D, POLFIS
DLC:  Ethertype  = 6003 (DECNET)
DLC:
DRP:  ----- DECNET Routing Protocol -----
DRP:
DRP:  Data length = 62
DRP:  Control Packet Format = 0B
DRP:              0... .... = no padding
DRP:              .000 .... = reserved
DRP:              .... 101. = Ethernet Router Hello Message
DRP:              .... ...1 = Control Packet Format
DRP:  Control Packet Type = 05
DRP:  Version Number  = 02
DRP:  ECO Number      = 00
DRP:  User ECO Number = 00
DRP:  ID of Transmitting Node = 31.458
DRP:       Information = 02
DRP:         0... .... = reserved
DRP:         .0.. .... = not blocking request
DRP:         ..0. .... = multicast traffic accepted
DRP:         ...0 .... = verification ok
DRP:         .... 0... = do not reject
DRP:         .... .0.. = no verification required
DRP:         .... ..10 = level 1 router
DRP:  Receive Block Size    = 1498
DRP:  Router's priority     = 64
DRP:  Area (reserved)       = 0
```

```
DRP:  Hello timer (seconds) = 15
DRP:  MPD (reserved)        = 0
DRP:  E-List length = 43
DRP:  Ethernet Name, reserved = 00000000000000
DRP:  Router/State length = 35
DRP:
DRP:  Router ID = 31.492
DRP:  Priority and State = C0
DRP:           1... .... = State known 2-way
DRP:           .100 0000 = Router's priority
DRP:
DRP:  Router ID = 31.501
DRP:  Priority and State = C0
DRP:           1... .... = State known 2-way
DRP:           .100 0000 = Router's priority
DRP:
DRP:  Router ID = 31.402
DRP:  Priority and State = C0
DRP:           1... .... = State known 2-way
DRP:           .100 0000 = Router's priority
DRP:
DRP:  Router ID = 31.401
DRP:  Priority and State = C0
DRP:           1... .... = State known 2-way
DRP:           .100 0000 = Router's priority
DRP:
DRP:  Router ID = 31.412
DRP:  Priority and State = C0
DRP:           1... .... = State known 2-way
DRP:           .100 0000 = Router's priority
DRP:

ADDR  HEX                                                ASCII
0000  AB 00 00 03 00 00 AA 00  04 00 CA 7D 60 03 3E 00  ...........}`.>.
0010  0B 02 00 00 AA 00 04 00  CA 7D 02 DA 05 40 00 0F  .........}...@..
0020  00 00 2B 00 00 00 00 00  00 00 23 AA 00 04 00 EC  ..+.......#.....
0030  7D C0 AA 00 04 00 F5 7D  C0 AA 00 04 00 92 7D C0  }......}......}.
0040  AA 00 04 00 91 7D C0 AA  00 04 00 9C 7D C0       .....}......}.
```

B.4.4 Routing di livello 1

Il seguente pacchetto è un distance vector di livello 1 trasmesso dal router 60.8 (nome DIDVX2), e riguardante quindi l'area 60, ai router ad esso adiacenti. Per ogni nodo dell'area 60 contiene una tripletta {Indirizzo, Hops, Costo}. I nodi noti al router DIDVX2 sono 32 e quindi il distance vector contiene 32 triplette.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 88 arrived at  00:48:07.9638; frame size is 294 (0126 hex)
      bytes.
DLC:  Destination = Multicast AB0000030000
DLC:  Source      = Station DECnet0008F0, DIDVX2
DLC:  Ethertype  = 6003 (DECNET)
DLC:
DRP:  ----- DECNET Routing Protocol -----
DRP:
DRP:  Data length = 278
DRP:  Control Packet Format = 07
DRP:              0... .... = no padding
DRP:              .000 .... = reserved
DRP:              .... 011. = Level 1 Routing Message
DRP:              .... ...1 = Control Packet Format
DRP:  Control Packet Type = 03
DRP:  Source Node      = 60.8
DRP:  Reserved field = 0
DRP:  RTGINFO count = 32
DRP:  Start ID = 480
DRP:  ID = 480   Hops = 31    Cost = 1023
DRP:  ID = 481   Hops = 31    Cost = 1023
DRP:  ID = 482   Hops = 31    Cost = 1023
DRP:  ID = 483   Hops = 31    Cost = 1023
DRP:  ID = 484   Hops = 31    Cost = 1023
DRP:  ID = 485   Hops = 31    Cost = 1023
DRP:  ID = 486   Hops = 01    Cost = 4
DRP:  ID = 487   Hops = 01    Cost = 4
DRP:  ID = 488   Hops = 31    Cost = 1023
DRP:  ID = 489   Hops = 31    Cost = 1023
DRP:  ID = 490   Hops = 01    Cost = 4
DRP:  ID = 491   Hops = 11    Cost = 44
DRP:  ID = 492   Hops = 31    Cost = 1023
DRP:  ID = 493   Hops = 31    Cost = 1023
DRP:  ID = 494   Hops = 31    Cost = 1023
DRP:  ID = 495   Hops = 31    Cost = 1023
DRP:  ID = 496   Hops = 31    Cost = 1023
DRP:  ID = 497   Hops = 31    Cost = 1023
DRP:  ID = 498   Hops = 01    Cost = 4
DRP:  ID = 499   Hops = 31    Cost = 1023
DRP:  ID = 500   Hops = 31    Cost = 1023
DRP:  ID = 501   Hops = 31    Cost = 1023
DRP:  ID = 502   Hops = 31    Cost = 1023
DRP:  ID = 503   Hops = 31    Cost = 1023
DRP:  ID = 504   Hops = 31    Cost = 1023
DRP:  ID = 505   Hops = 31    Cost = 1023
DRP:  ID = 506   Hops = 31    Cost = 1023
DRP:  ID = 507   Hops = 31    Cost = 1023
```

```
DRP:  ID = 508   Hops = 31    Cost = 1023
DRP:  ID = 509   Hops = 01    Cost = 4
DRP:  ID = 510   Hops = 01    Cost = 4
DRP:  ID = 511   Hops = 01    Cost = 4
DRP:
DRP:  Checksum = 0020
DRP:

ADDR  HEX                                                ASCII
0000  AB 00 00 03 00 00 AA 00  04 00 08 F0 60 03 16 01  ............`...
0010  07 08 F0 00 20 00 E0 01  FF 7F FF 7F FF 7F FF 7F  .... ...........
0020  FF 7F FF 7F 04 04 04 04  FF 7F FF 7F 04 04 2C 2C  ..............,,
0030  FF 7F FF 7F FF 7F FF 7F  FF 7F FF 7F 04 04 FF 7F  ................
0040  FF 7F FF 7F FF 7F FF 7F  FF 7F FF 7F FF 7F FF 7F  ................
0050  FF 7F 04 04 04 04 04 04  20 00 00 02 FF 7F FF 7F  ........ .......
0060  FF 7F FF 7F 04 04 FF 7F  20 20 FF 7F FF 7F FF 7F  ........  ......
0070  04 04 04 04 04 04 04 04  04 04 04 04 FF 7F FF 7F  ................
0080  FF 7F FF 7F FF 7F FF 7F  FF 7F FF 7F FF 7F 04 04  ................
0090  04 04 FF 7F FF 7F FF 7F  FF 7F 04 04 20 00 A0 02  ............ ...
00A0  FF 7F FF 7F FF 7F FF 7F  FF 7F FF 7F FF 7F 10 10  ................
00B0  FF 7F FF 7F FF 7F FF 7F  FF 7F FF 7F FF 7F FF 7F  ................
00C0  FF 7F 04 04 04 04 FF 7F  FF 7F FF 7F FF 7F FF 7F  ................
00D0  FF 7F FF 7F FF 7F FF 7F  FF 7F 04 04 FF 7F 04 04  ................
00E0  20 00 C0 02 FF 7F FF 7F  FF 7F FF 7F FF 7F FF 7F   ...............
00F0  FF 7F FF 7F FF 7F FF 7F  04 04 FF 7F FF 7F 04 04  ................
0100  20 20 FF 7F FF 7F FF 7F  48 48 FF 7F FF 7F FF 7F    ......HH......
0110  FF 7F FF 7F FF 7F FF 7F  FF 7F FF 7F FF 7F FF 7F  ................
0120  FF 7F FF 7F B0 2A                                  .....*
```

B.4.5 Routing di livello 2

Il seguente pacchetto è trasmesso dal router di area 31 e indirizzo 31.501 e contiene un distance vector di livello 2. Si tratta di 63 triplette {Area, Hops, Costo} che indicano la visibilità del router 31.501 sulle 63 aree DECnet (massimo teorico).

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 113 arrived at  00:48:08.5342; frame size is 152
      (0098 hex) bytes.
DLC:  Destination = Multicast AB0000030000
DLC:  Source      = Station DECnet00F57D
DLC:  Ethertype  = 6003 (DECNET)
DLC:
DRP:  ----- DECNET Routing Protocol -----
DRP:
DRP:  Data length = 136
```

```
DRP:  Control Packet Format = 09
DRP:              0... .... = no padding
DRP:              .000 .... = reserved
DRP:              .... 100. = Level 2 Routing Message
DRP:              .... ...1 = Control Packet Format
DRP:  Control Packet Type = 04
DRP:  Source Node      = 31.501
DRP:  Reserved field = 0
DRP:  RTGINFO count = 63
DRP:  Start Area = 1
DRP:  Area = 1     Hops = 31    Cost = 1023
DRP:  Area = 2     Hops = 31    Cost = 1023
DRP:  Area = 3     Hops = 31    Cost = 1023
DRP:  Area = 4     Hops = 31    Cost = 1023
DRP:  Area = 5     Hops = 31    Cost = 1023
DRP:  Area = 6     Hops = 31    Cost = 1023
DRP:  Area = 7     Hops = 31    Cost = 1023
DRP:  Area = 8     Hops = 31    Cost = 1023
DRP:  Area = 9     Hops = 31    Cost = 1023
DRP:  Area = 10    Hops = 31    Cost = 1023
DRP:  Area = 11    Hops = 31    Cost = 1023
DRP:  Area = 12    Hops = 31    Cost = 1023
DRP:  Area = 13    Hops = 31    Cost = 1023
DRP:  Area = 14    Hops = 31    Cost = 1023
DRP:  Area = 15    Hops = 31    Cost = 1023
DRP:  Area = 16    Hops = 31    Cost = 1023
DRP:  Area = 17    Hops = 31    Cost = 1023
DRP:  Area = 18    Hops = 31    Cost = 1023
DRP:  Area = 19    Hops = 31    Cost = 1023
DRP:  Area = 20    Hops = 31    Cost = 1023
DRP:  Area = 21    Hops = 31    Cost = 1023
DRP:  Area = 22    Hops = 31    Cost = 1023
DRP:  Area = 23    Hops = 31    Cost = 1023
DRP:  Area = 24    Hops = 31    Cost = 1023
DRP:  Area = 25    Hops = 31    Cost = 1023
DRP:  Area = 26    Hops = 31    Cost = 1023
DRP:  Area = 27    Hops = 31    Cost = 1023
DRP:  Area = 28    Hops = 31    Cost = 1023
DRP:  Area = 29    Hops = 31    Cost = 1023
DRP:  Area = 30    Hops = 31    Cost = 1023
DRP:  Area = 31    Hops = 00    Cost = 0
DRP:  Area = 32    Hops = 31    Cost = 1023
DRP:  Area = 33    Hops = 31    Cost = 1023
DRP:  Area = 34    Hops = 31    Cost = 1023
DRP:  Area = 35    Hops = 31    Cost = 1023
DRP:  Area = 36    Hops = 31    Cost = 1023
DRP:  Area = 37    Hops = 31    Cost = 1023
DRP:  Area = 38    Hops = 31    Cost = 1023
DRP:  Area = 39    Hops = 31    Cost = 1023
```

```
DRP:  Area = 40    Hops = 31    Cost = 1023
DRP:  Area = 41    Hops = 31    Cost = 1023
DRP:  Area = 42    Hops = 31    Cost = 1023
DRP:  Area = 43    Hops = 31    Cost = 1023
DRP:  Area = 44    Hops = 31    Cost = 1023
DRP:  Area = 45    Hops = 31    Cost = 1023
DRP:  Area = 46    Hops = 31    Cost = 1023
DRP:  Area = 47    Hops = 31    Cost = 1023
DRP:  Area = 48    Hops = 31    Cost = 1023
DRP:  Area = 49    Hops = 31    Cost = 1023
DRP:  Area = 50    Hops = 31    Cost = 1023
DRP:  Area = 51    Hops = 31    Cost = 1023
DRP:  Area = 52    Hops = 31    Cost = 1023
DRP:  Area = 53    Hops = 31    Cost = 1023
DRP:  Area = 54    Hops = 31    Cost = 1023
DRP:  Area = 55    Hops = 31    Cost = 1023
DRP:  Area = 56    Hops = 31    Cost = 1023
DRP:  Area = 57    Hops = 31    Cost = 1023
DRP:  Area = 58    Hops = 31    Cost = 1023
DRP:  Area = 59    Hops = 31    Cost = 1023
DRP:  Area = 60    Hops = 31    Cost = 1023
DRP:  Area = 61    Hops = 01    Cost = 20
DRP:  Area = 62    Hops = 31    Cost = 1023
DRP:  Area = 63    Hops = 31    Cost = 1023
DRP:
DRP:  Checksum = 8436
DRP:

ADDR  HEX                                              ASCII
0000  AB 00 00 03 00 00 AA 00  04 00 F5 7D 60 03 88 00 ...........}`...
0010  09 F5 7D 00 3F 00 01 00  FF 7F FF 7F FF 7F FF 7F ..}.?...........
0020  FF 7F FF 7F FF 7F FF 7F  FF 7F FF 7F FF 7F FF 7F ................
0030  FF 7F FF 7F FF 7F FF 7F  FF 7F FF 7F FF 7F FF 7F ................
0040  FF 7F FF 7F FF 7F FF 7F  FF 7F FF 7F FF 7F FF 7F ................
0050  FF 7F FF 7F 00 00 FF 7F  FF 7F FF 7F FF 7F FF 7F ................
0060  FF 7F FF 7F FF 7F FF 7F  FF 7F FF 7F FF 7F FF 7F ................
0070  FF 7F FF 7F FF 7F FF 7F  FF 7F FF 7F FF 7F FF 7F ................
0080  FF 7F FF 7F FF 7F FF 7F  FF 7F FF 7F FF 7F FF 7F ................
0090  14 04 FF 7F FF 7F 36 84                          ......6.
```

B.5 LAT

Il LAT (Local Area Transport) è il classico esempio di protocollo che non può essere trattato tramite router, ma solo tramite bridge, in quanto sprovvisto del livello 3. Infatti la busta LAT è contenuta direttamente nella busta Ethernet. In questo caso

il pacchetto LAT contiene un solo carattere "\", probabilmente proveniente da un terminale VT100 collegato ad un terminal server.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 29 arrived at  00:48:06.5073; frame size is 60 (003C hex)
      bytes.
DLC:  Destination = Station DEC   3761DF, CENSA1
DLC:  Source      = Station DEC   2A7463
DLC:  Ethertype  = 6004 (DEC LAT)
DLC:
LAT:  ----- Local Area Transport -----
LAT:
LAT:  Message type / flags = 02
LAT:             0000 00.. = Run
LAT:             .... ..1. = To host
LAT:             .... ...0 = No response requested
LAT:  Number of slots = 1
LAT:    Destination link ID = 5F01
LAT:         Source link ID = B802
LAT:        Sequence number = 71
LAT:  Acknowlegement number = CA
LAT:
LAT:  ----- Local Area Transport Data To Host (Slot 0) -----
LAT:
LAT:  Destination sublink ID = 26
LAT:       Source sublink ID = 21
LAT:  Data length = 1
LAT:  Slot type / Credits = 00
LAT:            0000 .... = Data
LAT:            .... 0000 = 0 Credits
LAT:  Data = "\"
LAT:

ADDR  HEX                                             ASCII
0000  08 00 2B 37 61 DF 08 00  2B 2A 74 63 60 04 02 01  ..+7a...+*tc`...
0010  01 5F 02 B8 71 CA 26 21  01 00 5C 4F 00 00 00 00  ._..q.&!..\O....
0020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0030  00 00 00 00 00 00 00 00  00 00 00 00              ............
```

B.6 ISO CLNS

I seguenti pacchetti appartengono al livello 3 ISO CLNS (connectionless). ISO CLNS è un insieme di protocolli che comprende ISO 8473 (Protocol ID = 81H), ISO 9542 ES-IS (Protocol ID = 82H) e ISO 10598 IS-IS (Protocol ID = 83H).

B.6.1 ISO Session Layer

Il seguente pacchetto, di tipo "give tokens", appartiene al Session OSI ed è imbustato in un pacchetto di Transport OSI (ISO_TP), imbustato in un pacchetto ISO 8473 (livello 3 OSI), imbustato in 802.2 (LLC), imbustato in 802.3. Si noti che ISO CLNS richiede sempre la presenza di LLC (SAP = FE) e quindi il pacchetto non può essere di tipo Ethernet, ma deve essere di tipo 802.3. A livello 3, gli indirizzi usati sono del tipo Local Character format, cioè stringhe di caratteri.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 8 arrived at  10:15:50.1488; frame size is 101 (0065 hex)
      bytes.
DLC:  Destination = Station U-B   38F200
DLC:  Source      = Station DG    010400
DLC:  802.3 length = 87
DLC:
LLC:  ----- LLC Header -----
LLC:
LLC:  DSAP = FE, SSAP = FE, Command, Unnumbered frame: UI
LLC:
CLNP: ----- ISO Network Layer -----
CLNP:
CLNP: Protocol ID = 81 (ISO Connectionless Network Protocol)
CLNP: Header length = 57
CLNP: Version / Protocol ID extension = 01
CLNP: Remaining PDU lifetime is 1.5 seconds
CLNP: Flags/type byte = 9C
CLNP:       1... .... = Segmentation permitted
CLNP:       .0.. .... = Last segment
CLNP:       ..0. .... = Error not reported if frame discarded
CLNP:       ...1 1100 = Data PDU
CLNP: Segment length = 84
CLNP: Checksum = 0000
CLNP: Destination address: "Ppci" (Local Character format)
CLNP:      Source address: "P10MAN2" (Local Character format)
CLNP: Data unit identifier = 0008
CLNP: Segment offset = 0
CLNP: Total length = 84
CLNP: Padding: 21 bytes
CLNP:
ISO_TP: ----- ISO Transport Layer -----
ISO_TP:
ISO_TP: Header length = 4
ISO_TP: TPDU type = F (Data)
ISO_TP: Destination reference = 0001
ISO_TP: EOT: Last TPDU of a sequence
```

```
ISO_TP: Send sequence number = 2
ISO_TP:
SESS: ----- ISO Session Layer -----
SESS:
SESS: SPDU type = 1 (Give Tokens)
SESS: Length of SPDU parameter field = 1
SESS:
SESS: Unknown parameter code = 0
SESS: Parameter length = 0
SESS: SPDU type = 0 (Exception Report)
SESS: SPDU type = 0 (Exception Report)
SESS: Length of SPDU parameter field = 4
SESS:
SESS: Unknown parameter code = 0
SESS: Parameter length = 22

ADDR  HEX                                                ASCII
0000  00 DD 00 38 F2 00 08 00  1B 01 04 00 00 57 FE FE  ...8.........W..
0010  03 81 39 01 03 9C 00 54  00 00 0A 50 70 63 69 00  ..9....T...Ppci.
0020  DD 00 38 F2 00 07 50 31  30 4D 41 4E 32 00 08 00  ..8...P10MAN2...
0030  00 00 54 CC 15 00 00 00  00 00 00 00 00 00 00 00  ..T.............
0040  00 00 00 00 00 00 00 00  00 00 04 F0 00 01 82 01  ................
0050  01 00 00 00 00 00 04 00  16 00 69 34 27 00 00 00  ..........i4'...
0060  00 8D 27 38 00                                   ..'8.
```

B.6.2 ISO SMB

Il seguente pacchetto è un SMB imbustato in ISO_TP, imbustato in ISO 8473, imbustato in IEEE 802.2, imbustato in IEEE 802.3. La sintassi usata per gli indirizzi di livello 3 è Local Binary format. Si noti che l'indirizzo di livello 2 MAC è contenuto nell'indirizzo di livello 3.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 2 arrived at  16:26:09.4999; frame size is 126 (007E hex)
      bytes.
DLC:  Destination = Station AT&T  010271
DLC:  Source      = Station AT&T  0100A9
DLC:  802.3 length = 112
DLC:
LLC:  ----- LLC Header -----
LLC:
LLC:  DSAP = FE, SSAP = FE, Command, Unnumbered frame: UI
LLC:
CLNP: ----- ISO Network Layer -----
CLNP:
```

```
CLNP: Protocol ID = 81 (ISO Connectionless Network Protocol)
CLNP: Header length = 49
CLNP: Version / Protocol ID extension = 01
CLNP: Remaining PDU lifetime is 3.0 seconds
CLNP: Flags/type byte = 9C
CLNP:       1... .... = Segmentation permitted
CLNP:       .0.. .... = Last segment
CLNP:       ..0. .... = Error not reported if frame discarded
CLNP:       ...1 1100 = Data PDU
CLNP: Segment length = 109
CLNP: Checksum = 0000
CLNP: Destination address: 490000000000000108006A010271FE01
      (Local Binary format)
CLNP: Source address: 490000000000000108006A0100A9FE01
      (Local Binary format)
CLNP: Data unit identifier = 0427
CLNP: Segment offset = 0
CLNP: Total length = 109
CLNP:
ISO_TP: ----- ISO Transport Layer -----
ISO_TP:
ISO_TP: Header length = 4
ISO_TP: TPDU type = 6 (Ack )
ISO_TP: Destination reference = 0002
ISO_TP: Next expected sequence number = 35
ISO_TP: Credit value = 7
ISO_TP:
ISO_TP: ----- ISO Transport Layer -----
ISO_TP:
ISO_TP: Header length = 4
ISO_TP: TPDU type = F (Data)
ISO_TP: Destination reference = 0002
ISO_TP: EOT: Last TPDU of a sequence
ISO_TP: Send sequence number = 82
ISO_TP:
SMB:  ----- SMB Delete File Command -----
SMB:
SMB:  Function = 06 (Delete File)
SMB:  Tree id      (TID) = 6000
SMB:  Process id   (PID) = 2D24
SMB:  File pathname = "\COPYDEST.4"
SMB:  Attribute flags = 0006
SMB:   .... ....  ..0. .... = File(s) not changed since last archive
SMB:   .... ....  ...0 .... = No directory file(s)
SMB:   .... ....  .... 0... = No volume label info
SMB:   .... ....  .... .1.. = System file(s)
SMB:   .... ....  .... ..1. = Hidden file(s)
SMB:   .... ....  .... ...0 = No read only file(s)
SMB:
```

```
ADDR  HEX                                               ASCII
0000  08 00 6A 01 02 71 08 00  6A 01 00 A9 00 70 FE FE  ..j..q..j....p..
0010  03 81 31 01 06 9C 00 6D  00 00 10 49 00 00 00 00  ..1....m...I....
0020  00 00 01 08 00 6A 01 02  71 FE 01 10 49 00 00 00  .....j..q...I...
0030  00 00 00 01 08 00 6A 01  00 A9 FE 01 04 27 00 00  ......j......'..
0040  00 6D 04 67 00 02 23 04  F0 00 02 D2 FF 53 4D 42  .m.g..#......SMB
0050  06 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0060  00 00 00 00 00 60 24 2D  00 00 00 00 01 06 00 0D  .....`$-........
0070  00 04 5C 43 4F 50 59 44  45 53 54 2E 34 00        ..\COPYDEST.4.
```

B.6.3 ISH

In questo caso ci troviamo in presenza di un pacchetto ISO 9542 ES-IS di tipo ISH (Intermediate System Hello). Si tratta cioè di un router OSI (IS: Intermediate System) che invia in multicast la sua identità agli End System (ES) affinché la inseriscano nella loro router cache locale.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 167 arrived at  00:48:10.0241; frame size is 60 (003C hex)
      bytes.
DLC:  Destination = Multicast 09002B000004
DLC:  Source      = Station DECnet00F57D
DLC:  802.3 length = 29
DLC:
LLC:  ----- LLC Header -----
LLC:
LLC:  DSAP = FE, SSAP = FE, Command, Unnumbered frame: UI
LLC:
CLNP: ----- ISO Network Layer -----
CLNP:
CLNP: Protocol ID = 82 (ISO Routing Exchange Protocol)
CLNP: Header length = 26
CLNP: Version / Protocol ID extension = 01
CLNP: PDU type: Intermediate System Hello (ISH)
CLNP: Holding time is 30 seconds
CLNP: Checksum = 0000
CLNP: Network entity title: 470020001FAA000400F57D00
      (ISO 6523-ICO Binary format)
CLNP: Suggested ES configuration timer = 600
CLNP:
DLC:  Frame padding= 17 bytes

ADDR  HEX                                               ASCII
0000  09 00 2B 00 00 04 AA 00  04 00 F5 7D 00 1D FE FE  ..+........}....
0010  03 82 1A 01 00 04 00 1E  00 00 0C 47 00 20 00 1F  ...........G. ..
```

```
0020  AA 00 04 00 F5 7D 00 C6  02 02 58 00 00 00 00 00  .....}....X.....
0030  00 00 00 00 00 00 00 00  00 00 00 00             ............
```

B.7 SNAP-PDU

Le SNAP-PDU sono delle particolari PDU di livello 2 LLC che servono ad imbustare nel campo dati LLC un protocollo non standard. LLC-DSAP e LLC-SSAP assumono il valore esadecimale AA e dopo il campo control sono inseriti 3 byte di OUI e 2 byte di protocol type.

B.7.1 AppleTalk

Nel pacchetto che segue vediamo che lo SNAP header contiene un vendor ID o OUI = 080007, corrispondente alla ditta Apple, e un protocol type o SNAP type = 809B, corrispondente al protocollo AppleTalk.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 30 arrived at  00:03:36.9210; frame size is 60 (003C hex)
      bytes.
DLC:  Destination = Multicast 090007FFFFFF
DLC:  Source      = Station 0080D300146D
DLC:  802.3 length = 43
DLC:
LLC:  ----- LLC Header -----
LLC:
LLC:  DSAP = AA, SSAP = AA, Command, Unnumbered frame: UI
LLC:
SNAP: ----- SNAP Header -----
SNAP:
SNAP: Vendor ID = 080007 (Apple)
SNAP: Type = 809B (AppleTalk)
SNAP: [35 byte(s) of data]
DLC:  Frame padding= 3 bytes

ADDR  HEX                                             ASCII
0000  09 00 07 FF FF FF 00 80  D3 00 14 6D 00 2B AA AA  ..........m.+..
0010  03 08 00 07 80 9B 00 23  00 00 00 00 03 A5 FF CB  .......#........
0020  01 01 01 03 A5 08 CB 03  84 80 03 E8 82 03 84 80  ................
0030  03 E8 82 03 E9 00 03 EB  00 00 00 00             ............
```

B.7.2 DEC MOP

Il MOP è il Maintenance Operation Protocol della Digital. Il suo header SNAP contiene un OUI = 08002B corrispondente a Digital Eq. Corp. e un protocol type = 6002 corrispondente al protocollo DEC MOP RC.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 6 arrived at  00:09:05.8256; frame size is 73 (0049 hex)
      bytes.
DLC:  Destination = Multicast AB0000020000
DLC:  Source      = Station DEC   3761DF, CENSA1
DLC:  802.3 length = 59
DLC:
LLC:  ----- LLC Header -----
LLC:
LLC:  DSAP = AA, SSAP = AA, Command, Unnumbered frame: UI
LLC:
SNAP: ----- SNAP Header -----
SNAP:
SNAP: Vendor ID = 08002B
SNAP: Type = 6002 (DEC MOP RC)
SNAP: [51 byte(s) of data]

ADDR  HEX                                             ASCII
0000  AB 00 00 02 00 00 08 00  2B 37 61 DF 00 3B AA AA .........+7a..;..
0010  03 08 00 2B 60 02 07 00  00 00 01 00 03 04 00 00 ...+`...........
0020  02 00 02 41 00 64 00 01  AA 90 01 01 01 07 00 06 ...A.d..........
0030  08 00 2B 37 61 DF 0A 00  10 C0 6D 0D D3 BF 7B CD ..+7a.....m...{.
0040  01 FF FF FF FF FF FF 3C  10                     .......<.
```

B.8 NOVELL NETWARE

Il protocollo Novell Netware usa a livello 3 il protocollo IPX derivato da Xerox XNS. La caratteristica atipica di IPX è quella di poter usare diversi tipi di imbustamento a livello 2. Novell può infatti sfruttare Ethernet, ed allora indica un protocol type uguale a 8137, ma può sfruttare anche 802.3 senza usare la busta 802.2.

Questa seconda possibilità è evidenziata nei due esempi che seguono.

B.8.1 Open file

Una busta 802.3 dovrebbe sempre contenere una busta 802.2. Questo nel caso di

IPX non si verifica, in quanto dopo il campo length della busta MAC 802.3 troviamo subito il pacchetto IPX. Questa eccezione viene discriminata in ricezione in quanto la busta IPX inizia sempre con 16 bit detti di checksum, ma posti sempre uguali a 1. Se la busta IPX venisse interpretata come busta LLC si avrebbe un LLC-SSAP uguale a FF, cioè broadcast che è chiaramente impossibile.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 5 arrived at  09:23:17.6181; frame size is 72 (0048 hex)
      bytes.
DLC:  Destination = Station 3Com  7AEC53
DLC:  Source      = Station 3Com  7AEC6E
DLC:  802.3 length = 58
DLC:
XNS:  ----- XNS Header -----
XNS:
XNS:  Checksum = FFFF
XNS:  Length = 57
XNS:  Transport control = 00
XNS:          0000 .... = Reserved
XNS:          .... 0000 = Hop count
XNS:  Packet type = 17 (Novell NetWare)
XNS:
XNS:  Dest   net = 00000001, host = 000000000001 (POLI-LAIB),
      socket = 1105 (NetWare Server)
XNS:  Source net = 00001000, host = 02608C7AEC6E, socket = 16387
      (4003)
XNS:
XNS:  ----- Novell Advanced NetWare -----
XNS:
XNS:  Request type = 2222 (Request)
XNS:  Seq no=14   Connection no=1    Task no=7
XNS:
NCP:   ----- Open File Request -----
NCP:
NCP:   Request code = 76
NCP:
NCP:   Dir handle = 03
NCP:   Search attribute flags = 06
NCP:                .... .1.. = System files allowed
NCP:                .... ..1. = Hidden files allowed
NCP:   Desired access rights = 13
NCP:               000. .... = Not defined
NCP:               ...1 .... = Exclusive (single-user mode)
NCP:               .... 0... = Allow others to open for writing
NCP:               .... .0.. = Allow others to open for reading
NCP:               .... ..1. = Open for writing
NCP:               .... ...1 = Open for reading
```

```
NCP:   File name = "/MGAI/DATA01.LOG"
NCP:
NCP:   [Normal end of NetWare "Open File Request" packet.]
NCP:

ADDR  HEX                                                ASCII
0000  02 60 8C 7A EC 53 02 60  8C 7A EC 6E 00 3A FF FF  .`.z.S.`.z.n.:..
0010  00 39 00 11 00 00 00 01  00 00 00 00 00 01 04 51  .9.............Q
0020  00 00 10 00 02 60 8C 7A  EC 6E 40 03 22 22 0E 01  .....`.z.n@."".
0030  07 00 4C 03 06 13 10 2F  4D 47 41 49 2F 44 41 54  ..L..../MGAI/DAT
0040  41 30 31 AE 4C 4F 47 49                          A01.LOGI
```

B.8.2 Login request

Il pacchetto seguente contiene una login request di un client Novell su un server Novell, imbustata in un protocollo NCP, imbustato in IPX, imbustato direttamente in 802.3. Si notino gli indirizzi IPX che sono gerarchici su due livelli (net e host).

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 9 arrived at  13:58:56.6606; frame size is 66 (0042 hex)
      bytes.
DLC:  Destination = Station 3Com  217692
DLC:  Source      = Station 3Com  119421
DLC:  802.3 length = 52
DLC:
XNS:  ----- XNS Header -----
XNS:
XNS:  Checksum = FFFF
XNS:  Length = 51
XNS:  Transport control = 00
XNS:          0000 .... = Reserved
XNS:          .... 0000 = Hop count
XNS:  Packet type = 17 (Novell NetWare)
XNS:
XNS:  Dest   net = 00217692, host = 02608C217692, socket = 1105
      (NetWare Server)
XNS:  Source net = 00217692, host = 02608C119421, socket = 16385
      (4001)
XNS:
XNS:  ----- Novell Advanced NetWare -----
XNS:
XNS:  Request type = 2222 (Request)
XNS:  Seq no=78   Connection no=4    Task no=1
XNS:
NCP:   ----- Login Request -----
```

```
NCP:
NCP:   Request/sub-function code = 23,0
NCP:
NCP:   Name = "DAN"
NCP:   Password = "GLIDE*"
NCP:
NCP:   [Normal end of NetWare "Login Request" packet.]
NCP:

ADDR  HEX                                                ASCII
0000  02 60 8C 21 76 92 02 60  8C 11 94 21 00 34 FF FF  .`.!v..`...!.4..
0010  00 33 00 11 00 21 76 92  02 60 8C 21 76 92 04 51  .3...!v..`.!v..Q
0020  00 21 76 92 02 60 8C 11  94 21 40 01 22 22 4E 04  .!v..`...!@."”N.
0030  01 00 17 00 0C 00 03 44  41 4E 06 47 4C 49 44 45  .......DAN.GLIDE
0040  2A 00                                            *.
```

B.9 VINES

Banyan Vines è un sistema operativo di rete concorrente di Novell Netware e di Microsoft LAN Manager.

B.9.1 Mail service

Il pacchetto seguente contiene in una busta Ethernet il livello 3 Vines IP, che contiene una busta VIPC (Vines Interprocess Communications Protocol), che contiene una busta Matchmaker, che contiene una busta di mail service.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 2 arrived at  15:08:02.7842; frame size is 110 (006E hex)
      bytes.
DLC:  Destination = Station 0074003D0000
DLC:  Source      = Station 3Com  177746
DLC:  Ethertype   = 0BAD (Banyan VINES)
DLC:
VIP: ----- VINES IP Header -----
VIP:
VIP: Checksum = FFFF (Null checksum)
VIP: Packet length = 96
VIP:
VIP: Transport control = 1F
VIP:         00.. .... = Unused
VIP:         ..0. .... = Do not return metric notification packet
```

```
VIP:         ...1 .... = Return exception notification packet
VIP:         .... 1111 = Hop count remaining (15)
VIP:
VIP: Protocol type = 1 (Interprocess Communications Protocol - VIPC)
VIP:
VIP: Destination network.subnetwork = 01000003.0001
VIP: Source network.subnetwork      = 001E86AF.80DE
VIP:
VIPC: ----- VINES IPC Header -----
VIPC:
VIPC: Source port      = 025D
VIPC: Destination port = 0004
VIPC:
VIPC: Packet type = 1 (Data)
VIPC:
VIPC: Control = 60
VIPC: 0... .... = Do not send immediate acknowledgment
VIPC: .1.. .... = End of message
VIPC: ..1. .... = Beginning of message
VIPC: ...0 .... = Do not abort current message
VIPC: .... 0000 = Unused
VIPC:
VIPC: Source connection ID       = 0111
VIPC: Destination connection ID = 002D
VIPC:
VIPC: Sequence number       = 7
VIPC: Acknowledgment number = 6
VIPC:
VIPC: Length = 62
VIPC:
MATCH: ----- VINES MATCHMAKER Header -----
MATCH:
MATCH: Packet type = 0 (Call)
MATCH:
MATCH: Transaction ID      = 0
MATCH: Program number      = 0
MATCH: Version number      = 1
MATCH: Procedure value     = 4
MATCH: Procedure arguments = 81 00 06 8A 00 1F . . .
MATCH:
MAIL: ----- VINES MAIL SERVICE Header -----
MAIL:
MAIL: Matchmaker packet type = 0 (Call)
MAIL: Procedure value = 4 (Any Changes?)
MAIL:
MAIL:

ADDR  HEX                                             ASCII
0000  00 74 00 3D 00 00 02 60  8C 17 77 46 0B AD FF FF  .t.=...`..wF....
```

```
0010  00 60 1F 01 01 00 00 03  00 01 00 1E 86 AF 80 DE  .`..............
0020  02 5D 00 04 01 60 01 11  00 2D 00 07 00 06 00 3E  .]...`...-.....>
0030  00 00 00 00 00 00 00 00  00 01 00 04 81 00 06 8A  ................
0040  00 1F 50 61 75 6C 20 4A  61 63 6B 73 6F 6E 40 33  ..Paul Jackson@3
0050  38 36 2B 50 43 58 40 43  6F 6E 76 65 72 67 65 6E  86+PCX@Convergen
0060  74 00 00 07 47 65 6E 65  72 61 6C 00 D1 BB        t...General...
```

B.10 BRIDGE PDU

Le Bridge PDU sono le PDU generate dal protocollo spanning tree dei bridge (capitolo 10). Nel caso in esame si tratta di una PDU 802.3 contenente una PDU 802.2 con LLC-SAP uguale a 42 esadecimale. La PDU 802.3 è inviata in multicast al MAC address 01-80-C2-00-00-00.

In questo caso la Bridge PDU è stata catturata su una LAN direttamente connessa al root bridge, come appare evidente dal fatto che gli indirizzi del root bridge (root bridge ID) e del bridge che ha trasmesso la PDU (sending bridge ID) sono identici.

In particolare la LAN su cui è stata catturata la PDU era connessa alla porta 3 del bridge.

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 1 arrived at  00:01:44.1485; frame size is 60 (003C hex)
      bytes.
DLC:  Destination = Multicast 0180C2000000
DLC:  Source      = Station DEC   28C724
DLC:  802.3 length = 38
DLC:
LLC:  ----- LLC Header -----
LLC:
LLC:  DSAP = 42, SSAP = 42, Command, Unnumbered frame: UI
LLC:
BPDU: ----- Bridge Protocol Data Unit Header -----
BPDU:
BPDU: Protocol Identifier = 0000
BPDU: Protocol Version    = 00
BPDU:
BPDU: BPDU Type == 00 (Configuration)
BPDU:
BPDU: BPDU Flags = 00
BPDU:  0... .... = Not Topology Change Acknowledgment
BPDU:  .000 0000 = Unused
BPDU:
BPDU: Root Identifier   = 0080.DEC   28C723
BPDU:   Priority        = 0080
```

```
BPDU:   MAC Address     = DEC   28C723
BPDU:
BPDU: Root Path Cost    = 0
BPDU:
BPDU: Sending Bridge Id = 0080.DEC   28C723.0003
BPDU:   Priority        = 0080
BPDU:   MAC Address     = DEC   28C723
BPDU:   Port            = 0003
BPDU:
BPDU:  Message Age          = 0.0     seconds
BPDU:  Information Lifetime = 1920.0
BPDU:  Root Hello Time      = 128.0
BPDU:  Forward Delay        = 1920.0
BPDU:
DLC:  Frame padding= 8 bytes

ADDR  HEX                                                ASCII
0000  01 80 C2 00 00 00 08 00  2B 28 C7 24 00 26 42 42 ........+(.$.&BB
0010  03 00 00 00 00 00 00 80  08 00 2B 28 C7 23 00 00 ..........+(.#..
0020  00 00 00 80 08 00 2B 28  C7 23 00 03 00 00 0F 00 ......+(.#......
0030  01 00 0F 00 00 00 00 00  00 00 00 00             ............
```

BIBLIOGRAFIA

[1] Network General, "Sniffer Manuals", Network General, Menlo Park CA (USA).

[2] Reynolds, J. Postel, "RFC 1340: Assigned Numbers", 07/10/1992.

[3] IBM, "Token-Ring Network: Architecture Reference", Pub. No. SC30-3374-01, second edition, August 1987.

[4] Cisco Systems, "Internetworking Technology Overview", Codice documento DOC-ITO13 78-1070-01, 1993.

[5] Cisco Systems, "Router Products: Configuration and Reference", Codice documento DOC-R9.1 78-0959-01, September 1992, Vol. I, II, III.

[6] Martin, J. Leben, "DECnet Phase V: An OSI Implementation", Digital Press, Bedford MA (USA), 1992.

[7] R. Perlman, "Interconnections: Bridges and Routers", Addison-Wesley, Reading MA (USA), 1992.

[8] Postel, J. Reynolds, "RFC 1042: A Standard for the Transmission of IP Datagrams over IEEE 802 Networks", February 1988.

Appendice C

GLOSSARIO

100BaseT: proposta, in corso di standardizzazione da parte del gruppo IEEE 802.3u, per una versione della rete locale Ethernet/IEEE 802.3 in grado di operare a 100 Mb/s.

100VG AnyLAN: proposta, in corso di standardizzazione da parte del gruppo IEEE 802.12, per una rete locale a 100 Mb/s in grado di trasportare trame Ethernet o Token Ring.

10Base2: standard IEEE/ISO 8802.3 per la trasmissione a 10 Mb/s su cavo coassiale RG58 da 50 Ω. Questo tipo di mezzo trasmissivo è spesso indicato come ThinWire cable o thinnet cable. Un segmento 10Base2 può essere lungo fino a 185 metri.

10Base5: standard IEEE/ISO 8802.3 per la trasmissione a 10 Mb/s sul cavo coassiale definito dalla specifica originale Ethernet "thick cable" a 50 Ω. Un segmento 10Base5 può essere lungo fino a 500 metri.

10BaseF: standard IEEE/ISO 8802.3 che racchiude tre standard per la trasmissione a 10 Mb/s su fibra ottica: 10BaseFP, 10BaseFB, 10BaseFL.

10BaseFB: standard IEEE/ISO 8802.3 per la trasmissione su fibra ottica che prevede l'uso di trasmissione sincrona per la realizzazione di dorsali in fibra ottica (FB significa Fiber Backbone) fra hub. Un segmento 10BaseFB può avere una lunghezza massima di 2000 metri.

10BaseFL: standard IEEE/ISO 8802.3 a 10 Mb/s che prevede l'uso di segmenti in fibra ottica (FL: Fiber Link) per la connessione di stazioni e hub. 10BaseFL è compatibile con lo standard FOIRL, ma può avere una lunghezza massima di 2000 metri.

10BaseFP: standard IEEE/ISO 8802.3 per la trasmissione a 10 Mb/s su fibra ottica che prevede l'uso di star ottiche passive. Un segmento che interconnette un MAU ad una star passiva può avere una lunghezza massima di 500 metri.

10BaseT: standard IEEE/ISO 8802.3 per la trasmissione a 10 Mb/s su un cavo UTP (Unshielded Twisted Pair) da 24 AWG. Un segmento 10BaseT può ammettere una distanza massima di 100 metri.

4B5B: tecnica di clock and data encoding tramite trasformazione basata su tabella di quartetti di bit in quintetti.

5B6B: tecnica di clock and data encoding tramite trasformazione basata su tabella di quintetti di bit in sestetti.

8B6T: tecnica di clock and data encoding tramite trasformazione basata su tabelle di ottetti in sequenze di sei simboli ternari.

AAL (ATM Adaptation Layer): insieme di protocolli che si appoggiano su ATM e forniscono vari servizi trasmissivi (voce, video, dati, ...) all'utente di una rete ATM.

ABM (Asynchronous Balanced Mode): modalità dei protocolli della famiglia HDLC per gestire una trasmissione connessa e full-duplex.

abstract interface: descrizione della semantica di una serie di servizi che un'entità in un livello funzionale del modello OSI fornisce all'utente dei servizi di quel livello. Una abstract interface non specifica i dettagli di implementazione, né descrive la sintassi che deve essere usata per implementare l'interfaccia.

ACK (acknowledgement): risposta inviata per indicare una corretta ricezione di un messaggio; gli acknowledgement possono essere presenti a vari livelli del modello di riferimento OSI (si veda anche confirmed service).

ACR (Attenuation to Cross-talk Ratio): rapporto tra il segnale ricevuto e il rumore indotto per diafonia.

address mask: maschera di 32 bit usata in TCP/IP per individuare l'indirizzo della sottorete.

advertisement: messaggio di tipo broadcast utilizzato per notificare a tutti i nodi la presenza di un dato servizio.

AFI (Authority and Format Identifier): nel modello di riferimento OSI, la prima delle due parti in cui è suddiviso il campo IDP dell'indirizzo NSAP; indica l'autorità che ha rilasciato l'indirizzo e il formato dello stesso.

AM (Amplitude Modulation): modulazione di ampiezza.

AMP PDU (Active Monitor Presence PDU): pacchetti che indicano la presenza dell'active monitor in una rete Token Ring.

ANSI (American National Standard Institute): ente di standardizzazione con attività nel settore delle rete locali; rappresenta gli Stati Uniti d'America nell'ISO.

API (Application Programming Interface): nel contesto delle reti, libreria di funzioni utilizzate per accedere da programma ai servizi di una data architettura.

APPC (Advanced Program-to-Program Communication): interfaccia di programmazione proposta dall'IBM per sviluppare applicativi distribuiti su architetture di rete SNA, APPN e TCP/IP.

APPN (Advanced Peer-to-Peer Networking): architettura di rete IBM, successiva ad SNA, che permette a calcolatori di ogni tipo di comunicare in modo paritetico su una topologia di rete arbitraria.

ARC (Active Retimed Concentrator): concentratore attivo IEEE 802.5.

architettura di rete: schema, organizzazione, insieme di regole che governano il progetto e le funzionalità delle componenti hardware e software di una rete di calcolatori.

architettura OSI (Open System Interconnection): architettura di rete proposta dall'ISO.

ARE (All Path Explorer packet): pacchetti che vengono trasmessi per esplorare i percorsi possibili per raggiungere una stazione token ring attraverso più reti interconnesse con bridge di tipo source routing.

area: partizione gerarchica di una rete determinata da un campo dell'indirizzo di livello 3.

ARP (Address Resolution Protocol): protocollo dell'architettura TCP/IP usato per convertire un indirizzo IP in un indirizzo di livello Data Link (spesso MAC). ARP lavora solo su una singola rete fisica ed è limitato a reti che supportano il broadcast hardware.

AS (Autonomous System): insieme di reti nell'architettura TCP/IP gestite da un'unica entità amministrativa; i router che le collegano utilizzano un protocollo di routing univoco.

ASCII (American Standard Code for Information Interchange): standard di codifica binaria a 7 o 8 bit per i caratteri alfanumerici e di controllo.

asincrona: tipo di trasmissione dati, a volte chiamata trasmissione start-stop , in cui la sincronizzazione tra trasmettitore e ricevitore viene ripristinata tramite un bit di start all'inizio di ogni carattere.

ASK (Amplitude-Shift Keying): modulazione di ampiezza usata nei modem.

attenuazione: perdita di energia di un segnale lungo un link.

ATM (Asynchronous Transfer Mode): standard CCITT per il trasferimento tramite celle di lunghezza fissa di informazioni di vario tipo (dati, voce, video, ecc.).

ATM switch: dispositivo multiporta in grado di commutare celle ATM.

ATMARP (ATM Address Resolution Protocol): versione modificata del protocollo ARP, operante su un server, in grado di gestire la corrispondenza tra indirizzi IP e indirizzi ATM.

AU (Access Unit): unità di accesso al bus DQDB.

AUI (Attachment Unit Interface) cable: cavo di interconnessione tra l'interfaccia Ethernet ed il transceiver, comunemente chiamato cavo drop.

AWG (American Wire Gauge): unità di misura dei cavi elettrici inversamente proporzionale alla sezione del cavo.

B-ISDN (Broadband ISDN): rete ISDN in grado di fornire servizi ad alta velocità sfruttando la tecnica ATM.

back-off: procedura con cui si ritenta una trasmissione in un MAC CSMA/CD.

backbone: dorsale di rete.

backbone collassato: dorsale di rete collassata in un centro stella realizzato mediante un concentratore o uno switch.

balun (BALunced-UNbalanced): dispositivo passivo o attivo per l'adattamento di una linea bilanciata ad una sbilanciata e viceversa.

banda: intervallo di frequenze trasmissibili da un canale; termine anche utilizzato per indicare l'intervallo di frequenze occupato da una trasmissione.

bandwidth: larghezza di banda.

baud: numero di simboli al secondo; i simboli possono essere binari, nel qual caso la velocità in baud coincide con la velocità in bit al secondo, oppure si possono utilizzare codifiche o modulazioni più complesse per rappresentare più bit con un solo simbolo.

BD (Building Distributor): locale tecnologico o armadio di distribuzione che costituisce il centro stella di edificio secondo la nomenclatura ISO/IEC 11801.

beacon process: processo di isolamento dei guasti in una LAN ad anello.

Bellman-Ford: nome alternativo utilizzato per indicare algoritmi di tipo distance vector.

BGP (Border Gateway Protocol): protocollo di routing, standardizzato da IETF, usato da un exterior router in un autonomous system per annunciare gli indirizzi delle reti appartenenti all'autonomous system stesso.

bilanciata: tecnica di trasmissione differenziale di segnali elettrici su coppie simmetriche.

bit stuffing: tecnica usata per delimitare le trame in modo non ambiguo e consentire la trasmissione di dati binari su una linea trasmissiva sincrona.

bit time: tempo dedicato alla trasmissione di un singolo bit; pari al reciproco della velocità trasmissiva espressa in b/s.

BLAN (Bridged LAN): insieme di LAN interconnesse da uno o più bridge.

BOM (Beginning Of Message): tipo di PDU nelle reti DQDB, SMDS e ATM.

BOOTP (BOOTstrap Protocol): protocollo appartenente all'architettura di rete TCP/IP per consentire ad una macchina diskless di effettuare il bootstrap su una rete locale.

BPDU (Bridge Protocol Data Unit): pacchetti del protocollo IEEE 802.1D che vengono scambiati tra i bridge per il calcolo dello spanning tree.

bps (bit per second): bit al secondo, anche abbreviato b/s; misura della velocità di una trasmissione dati.

BRI (Basic Rate Interface): l'interfaccia ISDN che offre due canali B (Bearer) a 64Kb/s e un canale D (Data) a 16Kb/s.

bridge: dispositivo attivo che opera a livello 2 OSI, usato per creare una LAN estesa unendo due o più LAN. Un bridge ritrasmette selettivamente i pacchetti tra le LAN cui è connesso.

bridge SR (Source Routing): bridge che ritrasmette solo pacchetti contenenti informazioni di source routing, cioè in cui il cammino è predeterminato dalla sorgente.

bridge SRT (Source Routing Transparent): bridge che può lavorare sia in modalità source routing che in modalità transparent bridging.

broadcast: trasmissione di un pacchetto a tutti i nodi di una rete.

brouter: apparato in grado di operare sia come bridge che come router in funzione dei protocolli e della configurazione.

buffer: area di memoria temporanea spesso utilizzata per compensare differenze di velocità tra trasmettitore e ricevitore.

BUS (Broadcast and Unknown Server): un server associato ad un servizio di emulazione LAN su ATM che svolge principalmente la funzione di gestione delle trame multicast/broadcast.

bus: topologia per reti locali in cui le stazioni sono collegate ad un singolo mezzo trasmissivo di tipo broadcast.

bypass relay: relay che permette di escludere un nodo non operativo in una rete ad anello.

cablaggio orizzontale: quella porzione di cablaggio strutturato che serve a collegare i posti di lavoro con gli armadi di piano.

cablaggio strutturato: infrastruttura per la trasmissione di segnali in ambito locale, realizzato contestualmente alla costruzione o ristrutturazione organica di un edificio, in conformità ai vigenti standard internazionali.

cablaggio verticale: quella porzione di cablaggio strutturato che realizza i collegamenti di dorsale.

campus: si veda comprensorio.

canale: parte di un sistema di comunicazione che connette una sorgente ad una o più destinazioni. Chiamato anche circuito, linea, link o path.

canale Bus-and-Tag: bus parallelo usato dai mainframe IBM per connettere dispositivi di rete, operante a circa 4MB/s.

canale ESCON: canale seriale in fibra ottica usato dai mainframe IBM per connettere dispositivi di rete.

capacità di canale: termine che esprime la massima velocità di trasmissione che può essere utilizzata su un canale.

cavo coassiale: tipo di cavo elettrico in cui un conduttore centrale è ricoperto da un isolante e poi circondato da uno schermo conduttore cilindrico il cui asse di simmetria coincide col conduttore centrale, da cui il termine "coassiale".

CCIR (Comité Consultatif International des Radiocomunications): la maggiore organizzazione mondiale nello sviluppo di standard relativi alle radiocomunicazioni e all'assegnazione delle frequenze..

CCITT (Comité Consultatif International de Telegraphie e Telephonie): la maggiore organizzazione mondiale nello sviluppo di standard relativi alla telefonia e ad altri servizi di comunicazione; fa parte dell'International Telecommunications Union (ITU).

CD (Campus Distributor): locale tecnologico o armadio di distribuzione situato nell'edificio centro stella di un comprensorio secondo la nomenclatura ISO/IEC 11801.

CDDI (Copper Distributed Data Interface): la realizzazione dello standard FDDI a 100 Mb/s in rame su doppino.

CDM (Code Division Multiplexing): tecnica per trasmettere più canali diversi su un unico mezzo trasmissivo utilizzando codici diversi.

CDMA (Code Division Multiple Access): condivisione di un unico mezzo trasmissivo da parte di più canali tramite tecnica CDM.

CDN (Canale Diretto Numerico): collegamento pubblico punto-punto o punto-multipunto sincrono a velocità comprese tra 4800 b/s e 2 Mb/s, realizzato con tecnologia digitale.

cella: pacchetto corto di lunghezza fissa (in ATM 53 ottetti).

CIDR (Classless Interdomain Routing): tecnica che consente ai router di raggruppare le informazioni di routing in modo da ridurre le dimensioni delle tabelle di instradamento.

circuit switching o commutazione di circuito: tecnica di commutazione per la trasmissione di dati digitali o di segnali analogici che consente a sistemi trasmissivi di creare un circuito temporaneo caratterizzato da basso ritardo e da banda costante.

circuito: termine generico usato nel routing DECnet per indicare il livello Data Link.

circuito virtuale: circuito, implementato tramite una rete a commutazione di pacchetto o di cella, che offre la simulazione di una connessione punto-punto fra due nodi.

circuito virtuale commutato: circuito virtuale creato dinamicamente su richiesta di un nodo tramite un protocollo di segnalazione, per la durata della trasmissione.

circuito virtuale permanente: circuito virtuale allocato permanentemente dal gestore della rete per la comunicazione tra due nodi.

claim token: processo di inizializzazione e generazione di un nuovo token; la stazione che vince questo processo emette il nuovo token.

CLNP (Connectionless Network Protocol): protocollo ISO di livello Network, non connesso, documentato in ISO 8473.

CLNS (**ConnectionLess-mode Network Service)**: servizio di livello Network in cui i pacchetti sono trasmessi da un protocollo non connesso (detto anche protocollo datagram); l'arrivo del pacchetto non è garantito, e le eventuali procedure di correzione degli errori devono essere implementate dai livelli superiori.

clock and data encoding: tecnica di codifica per fornire al ricevitore l'informazione di clock insieme a quella di dato utilizzando lo stesso canale trasmissivo.

CMIP (Common Management Information Protocol): protocollo dell'architettora OSI per la gestione degli apparati di rete.

collision domain: porzione di una rete CSMA/CD nella quale ha luogo una collisione se due o più entità MAC trasmettono contemporaneamente; le entità MAC separate da ripetitori sono nello stesso collision domain, quelle separate da bridge, router e gateway no.

collision handler: circuito di gestione delle collisioni.

collisione: trasmissione simultanea di due o più stazioni su un mezzo trasmissivo condiviso.

COM (Continuation Of Message): tipo di PDU nelle reti DQDB, SMDS e ATM.

commutazione di circuito: si veda circuit switching.

commutazione di pacchetto: si veda packet switching.

comprensorio: singolo appezzamento di suolo privato oppure più appezzamenti di suolo privato separati da suolo pubblico, ma collegati da opere aventi carattere permanente (es. sottopassi).

concentratore: nelle reti locali cablate a stella l'apparato che funge da centro stella.

confirm: nel modello di riferimento OSI, nei protocolli che prevedono acknowledge, primitiva di servizio attivata per confermare al mittente la ricezione di una PDU (si veda anche indication).

confirmed service: servizio con cui il richiedente il servizio viene informato dall'entità remota di pari livello del successo o insuccesso della richiesta di servizio.

connection-mode service: servizio affidabile realizzato tipicamente tramite un protocollo connesso.

connectionless-mode service: servizio realizzato tramite un protocollo non connesso che non garantisce la consegna delle PDU.

CONS (COnnection-mode Network Service): servizio affidabile di livello Network in cui le PDU sono scambiate tramite un protocollo connesso.

controllo di flusso: tecnica che tende a evitare o a risolvere congestioni di nodi sospendendo o riducendo l'immissione di nuovi dati sui mezzi trasmissivi.

COS (Class Of Service): sigla che indica la qualità del servizio nelle architetture SNA e APPN.

CPT (Collision Presence Test): si veda Signal Quality Error Test.

CRC (Cyclic Redundancy Code): stringa binaria calcolata tramite opportune funzioni algebriche ed utilizzata per rilevare gli errori di trasmissione.

cross-talk: si veda diafonia.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance): protocollo di livello MAC per l'accesso multiplo ad un mezzo condiviso con meccanismo di contesa iniziale per evitare le collisioni dei pacchetti di dato. Utilizzato nelle reti wireless e nella rete LocalTalk (Apple Macintosh).

CSMA/CD (Carrier Sense Multiple Access with Collision Detection): protocollo di livello MAC per l'accesso multiplo ad un mezzo condiviso con meccanismo di contesa tra i pacchetti di dato. Utilizzato nella rete Ethernet.

cut-through: metodo di commutazione in cui la ritrasmissione di un pacchetto inizia mentre è ancora in corso la sua ricezione.

DAC (Dual Attachment Concentrator): concentratore FDDI che funge da centro stella, principalmente per stazioni SAS, e da elemento di collegamento con il doppio anello controrotante.

DAS (Dual Attachment Station): stazione FDDI che si collega al doppio anello controrotante tramite due connessioni fisiche, e pertanto fault tolerant.

Data Link: secondo livello del modello di riferimento OSI; si occupa della trasmissione di trame tra nodi fisicamente adiacenti.

datagram: pacchetti trasmessi tramite un protocollo non connesso.

datagram service: si veda connectionless-mode service.

dB (decibel): misura della potenza di un segnale relativamente ad un altro segnale; il valore in decibel viene calcolato come 10 volte il logaritmo del rapporto fra le potenze dei due segnali, oppure come 20 volte il logaritmo del rapporto fra le ampiezze (tensioni o correnti).

DCC (Data Country Code): uno dei possibili formati dell'indirizzo OSI NSAP, la cui gestione è a cura del rappresentante nazionale dell'ISO (ad esempio, l'UNINFO per l'Italia).

DCE (Data Communication Equipment): termine usato dagli standard CCITT per indicare i dispositivi che fungono da punti di accesso ad una rete pubblica; i DCE, tipicamente modem, si collegano ai DTE.

DDCMP (Digital Data Communication Message Protocol): protocollo di livello Data Link utilizzato nelle reti geografiche dall'architettura DECnet.

DECnet: nome originale dell'architettura di rete della Digital Equipment Corp. ed ora parte della più generale DNA (Digital Network Architecture).

diafonia: fenomeno di accoppiamento indesiderato tra due canali trasmissivi.

DIS (Draft International Standard): bozza di standard internazionale ISO che ne precede la versione finale.

distance vector: algoritmo adattativo e distribuito per il calcolo delle tabelle di instradamento basato su un processo iterativo di scambio delle stesse tra router adiacenti; talvolta anche chiamato algoritmo di Bellman-Ford.

DLCI (Data Link Connection Identifier): un campo nella trama Frame Relay che identifica la connessione logica cui essa appartiene.

DNA (Digital Network Architecture): architettura di rete proprietaria della Digital Equipment Corp., anche nota come DECnet.

DNS (Domain Name Server): servizio per la gestione e traduzione da nomi a indirizzi e viceversa nell'architettura di rete TCP/IP.

dominio di routing: termine generico che indica una partizione gerarchica della rete contenente un insieme di nodi e di router; i router condividono le stesse informazioni di routing, calcolano le tabelle utilizzando lo stesso algoritmo, e sono gestiti da un amministratore comune.

doppino: termine indicante una coppia di fili elettrici ritorti, spesso usato anche per indicare cavi a più coppie.

DQDB (Distributed Queue Dual Bus): standard IEEE 802.6 per reti metropolitane.

drop cable: si veda AUI cable.

DRP (DECnet Routing Protocol): protocollo di livello Network utilizzato nell'architettura di rete DECnet fase IV.

DSAP (Destination Service Access Point): sigla usata per indicare l'indirizzo del destinatario nel modello di riferimento OSI.

DSP (Digital Signal Processor): microprocessore specializzato nell'elaborazione digitale dei segnali, utilizzato nei modem di nuova generazione.

DSP (Domain Specific Part): nel modello di riferimento OSI, la seconda delle due parti in cui è suddiviso l'indirizzo NSAP.

DSU (Data Segmentation Unit): dispositivo che realizza funzioni di segmentazione e riassemblaggio di una trama in celle.

DTE (Data Terminal Equipment): termine usato negli standard CCITT per indicare un dispositivo di elaborazione, come un computer o un terminale; i DTE si collegano normalmente ai DCE.

DXI (Data eXchange Interface): l'interfaccia tra un router e un dispositivo esterno DSU.

E.163: standard per i piani di numerazione per le reti telefoniche.

E.164: standard per i piani di numerazione per le reti ISDN.

E1 (European 1): trama del primo livello della gerarchia PDH europea con velocità di 2 Mb/s.

E3 (European 3): trama del terzo livello della gerarchia PDH europea con velocità di 34 Mb/s.

E4 (European 4): trama del quarto livello della gerarchia PDH europea con velocità di 140 Mb/s.

early token release: tecnica di rilascio anticipato del token utilizzato nella rete Token Ring a 16 Mb/s e in FDDI.

EBCDIC (Extended Binary Coded Decimal Interchange Code): codice binario su 8 bit utilizzato principalmente dalle apparecchiature IBM per rappresentare caratteri alfanumerici e di controllo.

ECMA (European Computer Manufacture Association): associazione europea di costruttori di calcolatori con attività nel campo della standardizzazione.

EF (Entrance Facility): punto di ingresso delle dorsali di comprensorio secondo la nomenclatura EIA/TIA 568.

EGP (Exterior Gateway Protocol): protocollo di routing, standardizzato da IETF, usato da un exterior router in un autonomous system per annunciare gli indirizzi delle reti appartenenti all'autonomous system stesso.

EIA (Electronic Industries Association): associazione di industrie elettroniche con attività nel campo della standardizzazione.

EMC (Electro Magnetic Compatibility): capacità di apparati elettronici suscettibili a disturbi elettromagnetici ed al contempo sorgenti dei medesimi di funzionare correttamente nello stesso ambiente.

end node: termine usato per indicare a un nodo che può agire solamente come una sorgente o destinazione finale di dati dell'utente e che non effettua le funzioni di routing.

entità: nel modello di riferimento OSI, un elemento attivo in un dato livello.

EOM (End Of Message): tipo di PDU nelle reti DQDB, SMDS e ATM.

ER (Equipment Room): locale tecnologico secondo la nomenclatura EIA/TIA 568.

ES (End System): termine OSI usato per indicare a un nodo che può agire solamente come una sorgente o destinazione finale di dati dell'utente e che non effettua le funzioni di routing.

ES-IS (End System to Intermediate System protocol): protocollo OSI, specificato in ISO 9542, per il neighbor greetings fra router ed end node e per associare gli indirizzi del livello Network agli indirizzi del livello di Data Link.

Ethernet: rete locale CSMA/CD; termine a volte usato genericamente per riferirsi ad una LAN IEEE 802.3.

Ethernet Full-Duplex: utilizzo di due collegamenti Ethernet in parallelo (normalmente tra due bridge o tra due switch) per permettere la trasmissione contemporanea nei due sensi.

Ethernet Switch: dispositivo multiporta in grado di commutare trame Ethernet/IEEE 802.3.

Ethernet Switching: tecnica per realizzare reti locali Ethernet/IEEE 802.3 che utilizza Ethernet switch per aumentare la capacità trasmissiva globale della rete.

F.69: standard per i piani di numerazione per le reti telex.

FCS (Frame Check Sequence): informazione di controllo per la verifica della correttezza di una PDU basata su CRC.

FD (Floor Distributor): armadio di piano secondo la nomenclatura ISO/IEC 11801.

FDDI (Fiber Distributed Data Interface): standard per LAN a 100 Mb/s in fibra ottica e topologia ad anello con elevate caratteristiche di tolleranza ai guasti; attualmente disponibile anche per mezzi trasmissivi in rame.

FDM (Frequency Division Multiplexing): tecnica per trasmettere più canali sullo stesso mezzo trasmissivo mediante traslazione in frequenza.

FDMA (Frequency Division Multiple Access): condivisione di un unico mezzo trasmissivo da parte di più canali tramite tecnica FDM.

FEP (Front End Processor): computer per la gestione delle comunicazioni nell'architettura di rete IBM/SNA; svolge principalmente funzionalità di routing.

FEXT (Far End Cross-Talk) o telediafonia: diafonia tra le coppie di un doppino misurata dalla parte opposta al trasmettitore.

flag: nei protocolli di Data Link della famiglia HDLC è un ottetto (01111110) che indica l'inizio e la fine di una trama.

flooding: algoritmo di routing non adattativo in cui un router propaga i pacchetti a tutti i router adiacenti.

flow control: si veda controllo di flusso.

FM (Frequency Modulation): modulazione di frequenza.

FOIRL (Fiber Optic Inter Repeater Link): standard facente parte dell'IEEE 802.3 per la trasmissione su fibra ottica.

frame: si veda trama.

frame relay: standard per la realizzazione di reti a commutazione di pacchetto pubbliche o private, basato su un protocollo di livello Data Link connesso su cui vengono definiti dei circuiti virtuali permanenti.

framing: operazione per delimitare l'inizio e la fine di una trama prima di effettuarne la trasmissione sul mezzo fisico.

FSK (Frequency-Shift Keying): modulazione di frequenza usata nei modem.

FTAM (File Transfer, Access, and Management): protocollo di livello applicativo nel modello di riferimento OSI, per accedere e trasferire file di dati, tra sistemi aperti, in un ambiente di rete eterogeneo.

FTP (File Transfer Protocol): l'architettura di rete TCP/IP per il file transfer.

FTP (Foiled Twisted Pair): cavo, normalmente a quattro coppie, avente uno schermo globale realizzato con foglio di alluminio.

full duplex: modalità di trasmissione bidirezionale simultanea.

functional address o indirizzo funzionale: tipo di indirizzamento multicast utilizzato nello standard IEEE 802.5.

G.703: standard CCITT a livello Fisico per l'interconnessione ad alta velocità tra DTE e DCE.

gabbia di Faraday: struttura metallica con capacità schermante per i disturbi elettromagnetici.

GARR (Gruppo Armonizzazione Reti per la Ricerca): organismo patrocinato dal MURST (Ministero per l'Università e la Ricerca Scientifica e Tecnologica) per la gestione e lo sviluppo della rete omonima.

gateway: dispositivo usato per connettere due architetture di rete diverse mediante la conversione di alcuni protocolli applicativi dell'una in quelli omologhi dell'altra.

half duplex: modalità di trasmissione bidirezionale non simultanea nei due sensi; in ogni istante la comunicazione è monodirezionale.

Hayes: linguaggio di comandi per i modem.

HDLC (High-level Data Link Control): protocollo di livello Data Link utilizzato nelle WAN derivato da SDLC e capostipite di una famiglia di protocolli a cui appartengono LAP-B, LAB-D, LAP-F e LLC.

header: parte iniziale di una PDU che contiene informazioni di controllo.

heartbeat: si veda Signal Quality Error test.

hop: attraversamento di un link, spesso usato come metrica a livello Network.

host: nell'architettura di rete TCP/IP, sinonimo di end system.

HPR (High Performance Routing): recente versione di APPN che introduce un algoritmo di routing ottimizzato per canali trasmissivi ad alte prestazioni.

hub: concentratore per LAN, normalmente con funzionalità di ripetitore.

Hz (Hertz): unità di misura della frequenza pari al numero di eventi al secondo.

IC (Intermediate Crossconnect): locale tecnologico o armadio di distribuzione che è il centro stella di un edificio secondario secondo la nomenclatura EIA/TIA 568.

ICMP (Internet Control Message Protocol): nell'architettura di rete TCP/IP, protocollo ausiliario di livello Network utilizzato per funzioni di neighbor greetings e per riportare anomalie nell'instradamento dei pacchetti.

IDI (Initial Domain Identifier): nel modello di riferimento OSI, la seconda delle due parti in cui è suddiviso il campo IDP dell'indirizzo NSAP.

IDP (Initial Domain Part): nel modello di riferimento OSI, la prima delle due parti in cui è suddiviso l'indirizzo NSAP.

IDRP (InterDomain Routing Protocol): protocollo di routing tra domini OSI di tipo distance vector derivato da BGP.

IEC (International Electrotechnical Commission): commissione dell'Unione Europea con attività nel settore della standardizzazione.

IEEE (Institute of Electrical and Electronics Engineers): associazione internazionale anche con attività nel campo della standardizzazione delle reti locali.

IETF (Internet Engineering Task Force): gruppo di lavoro dell'ISOC che cura la standardizzazione e l'evoluzione dell'architettura di rete TCP/IP.

IFS (Inter Frame Spacing): si veda Inter Packet Gap.

IGP (Interior Gateway Protocol): termine generico applicato ad ogni protocollo usato per propagare informazioni di raggiungibilità e di routing all'interno di un sistema autonomo; benché non esista un IGP standard per Internet, RIP è fra i più comuni.

IGRP (Interior Gateway Routing Protocol): un protocollo di routing di tipo IGP sviluppato da CISCO secondo la filosofia distance vector.

IMP (Interface Message Processor): vecchio nome dei commutatori di pacchetto usati in ARPANET, ora definiti più propriamente router.

impedenza: nei mezzi elettrici, relazione tra tensione e corrente in funzione della frequenza.

InARP (Inverse ARP): sinonimo di RARP.

indication: nel modello di riferimento OSI, primitiva di servizio attivata sul nodo di destinazione a fronte della ricezione di una PDU (si veda anche request).

indirizzo: stringa che identifica univocamente un'entità di rete.

indirizzo Internet: indirizzo a 32 bit assegnato alle interfacce degli host e dei router che utilizzano l'architettura di rete TCP/IP; lo si scrive come quattro numeri decimali separati da punti.

indirizzo MAC: indirizzo di livello Data Link, sottolivello MAC, usato nelle reti locali, tipicamente lungo 48 bit e assegnato dal produttore della scheda di rete; lo si scrive come sei coppie di cifre esadecimali.

Integrated IS-IS (precedentemente detto **Dual IS-IS**): un protocollo di routing basato sull'IS-IS di OSI, ma in grado di supportare anche IP e altri protocolli; integrated IS-IS propaga contemporaneamente le informazioni di raggiungibilità di tutti i protocolli tramite lo stesso LSP.

inter-area routing: operazione effettuata dai router di frontiera quando instradano un pacchetto tra aree diverse.

Internet: la più grande rete di calcolatori al mondo, basata sull'architettura di rete TCP/IP.

internet protocol suite: l'architettura di rete normalmente nota con il nome di TCP/IP.

intra-area routing: operazione effettuata dai router quando instradano un pacchetto all'interno della stessa area.

IP (Internet Protocol): nell'architettura di rete TCP/IP, il protocollo dati di livello Network.

IPG (Inter Packet Gap): intervallo di tempo minimo tra due trame Ethernet.

IPX (Internetwork Packet eXchange): un protocollo di livello Network utilizzato da Novell e simile a XNS e IP.

IS (Intermediate System): **t**ermine OSI che indica un nodo (tipicamente un router) che ha capacità di instradare messaggi a livello 3 verso altri nodi.

IS-IS (Intermediate System to Intermediate System protocol): nell'architettura di rete OSI, il protocollo di livello Network per il calcolo delle tabelle di instradamento all'interno di un dominio.

ISDN (Integrated Services Digital Network): rete pubblica commutata digitale.

ISO (International Standard Organization): principale organismo di standardizzazione mondiale di cui fanno parte gli organismi di standardizzazione nazionali quali l'ANSI per gli USA e l'UNINFO per l'Italia.

ISO/IEC DIS 11801: bozza di standard internazionale per il cablaggio degli edifici commerciali approvata nel mese di luglio 1994.

ISOC (Internet SOCiety): organizzazione per lo sviluppo della rete Internet e dell'architettura di rete TCP/IP.

ISODE (ISO Development Environment): ambiente per lo sviluppo di applicazioni OSI su TCP/IP.

ITU (International Telecommunication Union): agenzia delle Nazioni Unite con attività principale nel campo della standardizzazione.

ITU-R (ITU Radiocommunications): nuova denominazione del CCIR.

ITU-T (ITU Telecommunications): nuova denominazione del CCITT.

jabber error: in IEEE 802.3 errore dovuto ad una trama la cui lunghezza eccede la massima consentita.

jamming sequence: in IEEE 802.3 sequenza illegale di bit per segnalare un'avvenuta collisione.

jitter: scostamento del bit time rispetto al valore nominale.

label swapping: tecnica di instradamento utilizzatta nei protocolli connessi.

LAN (Local Area Network): sistema di comunicazione che permette ad apparecchiature indipendenti di comunicare tra di loro entro un'area delimitata utilizzando un canale fisico a velocità elevata e con basso tasso di errore.

LAN emulation: tecnica per l'emulazione delle funzionalità di una LAN IEEE 802.3 o IEEE 802.5 su una rete ATM.

LAP (Link Access Procedure): termine generico che indica un protocollo della famiglia HDLC.

LAP-B (LAP Balanced): protocollo LAP usato nelle reti X.25.

LAP-D (LAP Data): protocollo LAP usato nelle reti ISDN.

LAP-F (LAP Frame): protocollo LAP usato nelle reti Frame Relay.

LAT (Local Area Transport): protocollo dell'architettura DNA utilizzato in ambito locale per il collegamento tra terminal server e calcolatori.

LEC (LAN Emulation Client): una stazione ATM che può emulare le funzionalità di una stazione IEEE 802.3 o IEEE 802.5.

LECS (LAN Emulation Configuration Server): un processo software associato ad una rete ATM che permette di configurare l'emulazione di una o più LAN IEEE 802.3 o IEEE 802.5.

LEN (Low Entry Network): particolare tipo di nodo nell'architettura APPN.

LES (LAN Emulation Server): un processo software associato ad un servizio di emulazione LAN su ATM che svolge principalmente la funzione di traduzione degli indirizzi MAC in indirizzi ATM.

link: canale tra due nodi.

link state: tecnica di calcolo delle tabelle di instradamento in cui un router comunica a tutti gli altri router della rete lo stato dei link a lui direttamente connessi tramite un pacchetto LSP.

link test fail: negli standard 10BaseF e 10BaseT, l'indicazione che non viene ricevuto alcun segnale sul canale di ricezione.

LIS (Logical IP Subnetwork): sottorete IP definita tramite il parametro netmask; ad ogni LIS è associata una rete fisica che permette a tutte le stazioni connesse a quella LIS di comunicare tra loro direttamente (senza utilizzare router).

LLC (Logical Link Control): nello standard IEEE 802 il sottolivello superiore del livello Data Link; protocollo appartenente alla famiglia HDLC.

lobo: nelle reti ad anello cablate a stella, la connessione tra una stazione e il concentratore.

LSP (Link State Packet): pacchetto generato da un protocollo di calcolo delle tabelle di instradamento di tipo link state; contiene la lista dei nodi adiacenti.

LU (Logical Unit): punto di accesso alla rete associato ad un utente nell'architettura SNA.

LU 6.2: il tipo di LU utilizzato per realizzare sessioni peer-to-peer nell'architettura SNA.

MAC (Medium Access Control): sottolivello inferiore del livello di Data Link che è responsabile di eseguire le procedure che gestiscono la condivisione del mezzo trasmissivo; il sottolivello MAC fornisce servizi non connessi al sottolivello di Logical Link Control.

MAC-Bridge: bridge che operano al sottolivello MAC del livello 2.

Main Crossconnect (MC): locale tecnologico o armadio di distribuzione che è il centro stella del comprensorio ed è situato nell'edificio principale secondo la nomenclatura EIA/TIA 568.

MAN (Metropolitan Area Network): rete metropolitana per collegamenti ad alta velocità (da centinaia di Mb/s al secondo fino a Gb/s) su un'area urbana.

Manchester: codifica a livello fisico che combina i valori dei bit di dato con le transizioni di un segnale di clock; usata in Ethernet e Token Ring.

master: nei sistemi trasmissivi punto-multipunto, la stazione che arbitra il canale mediante operazioni di polling.

MAU (Medium Attachment Unit): transceiver, cioè elemento di connessione al mezzo trasmissivo in Ethernet e IEEE 802.3.

MAU (Multistation Access Unit): concentratore che funge da centro stella in Token Ring e IEEE 802.5.

MDI (Medium Dependent Interface): interfaccia a livello Fisico dipendente dal mezzo trasmissivo usato.

MIB (Management Information Base): formato per la definizione dei parametri di gestione di un apparato di rete utilizzato dal protocollo SNMP.

MIC (Medium Interface Connector): connettore tra mezzo trasmissivo e interfaccia.

MLT-3: schemi di clock and data encoding utilizzanti simboli ternari.

MODEM (Modulatore-DEModulatore): dispositivo per la trasmissione di dati digitali su canali trasmissivi analogici (tipicamente telefonici) tramite opportuna modulazione (ad esempio FSK, QAM, DPSK).

multicast: trasmissione di un pacchetto a un gruppo di nodi di una rete.

multidrop o punto-multipunto: tipo di canale a cui sono connesse più stazioni di cui una ne arbitra l'utilizzo svolgendo le operazioni di master.

N-ISDN (Narrowband ISDN): ISDN classico, in contrapposizione a B-ISDN.

NAU (Network Addressable Unit): entità di rete indirizzabile nell'architettura SNA.

NAUN (Nearest Active Upstream Neighbor): nelle reti ad anello, l'identificativo della più vicina stazione attiva a monte.

NBMA (Non Broadcast Multiple Access): rete ad accesso multiplo che non fornisce la possibilità di trasmettere un pacchetto a tutte le stazioni in modalità broadcast; le reti X.25 sono un esempio di reti NBMA.

neighbor greetings: definizione spesso usata per indicare i protocolli di tipo ES-IS.

neighbor notification: nelle reti ad anello, processo attivato periodicamente per identificare il NAUN.

NET (Network Entity Title): nell'architettura di rete OSI, l'indirizzo NSAP con il campo SEL posto uguale a zero.

NETBEUI (NETBios Extended User Interface): protocollo per la realizzazione di reti di PC, appartenente all'architettura SNA ed usato come protocollo standard nelle reti Microsoft.

NetBIOS (Network Basic Input Output System): API standard per le reti di personal computer.

NETID (NETwork IDentification): identificatore di una sottorete nell'architettura APPN.

NEXT (Near End Cross-Talk) o paradiafonia: diafonia tra le coppie di un doppino misurata dalla parte del trasmettitore.

NFS (Network File System): protocollo sviluppato da SUN Microsystems che si appoggia sull'architettura di rete TCP/IP e consente ad un insieme di elaboratori di condividere i file system.

NHRP (Next Hope Resolution Protocol): un protocollo simile al protocollo ARP, che consente di gestire in modo più efficace il routing IP su reti NBMA (ad esempio, reti ATM).

NIR (Next to Insertion loss Ratio): termine utilizzato nello standard IEEE 802.5 per indicare l'ACR.

nodi adiacenti: nodi che sono raggiungibili in un singolo hop.

nodo: termine usato in DNA per riferirsi ad un dispositivo che contiene almeno una istanza del livello Network e dei sottostanti livelli Data Link e Fisico. È sinonimo del termine OSI "system".

nome descrittivo: nello standard X.500, nome che identifica un'entità specificando informazioni sugli attributi di tale oggetto.

nome primitivo: stringa di caratteri che identificano univocamente un'entità.

notazione puntata: rappresentazione di un numero intero su 32 bit tramite quattro numeri decimali separati da punti ciascuno dei quali rappresenta il valore di un ottetto. Utilizzato per gli indirizzi TCP/IP.

NRM (Normal Response Mode): nei protocolli della famiglia HDLC la modalità operativa master-slave half-duplex.

NRZ/NRZI (Non Return to Zero / Non Return to Zero Inverted): schemi di clock and data encoding utilizzanti simboli binari**.**

NSAP (Network Service Access Point): indirizzo di livello Network nell'architettura OSI.

NSP (Network Service Protocol): protocollo di livello Transport utilizzato nell'architettura di rete DECnet.

NSP (Network Service Protocol): protocollo proprietario della Digital Equipment Corp. per il livello di trasporto usato in DECNET fase IV.

NT (Network Termination): terminazione di rete ISDN; esiste in due versioni: NT1 e NT2.

null modem: cavo di interfaccia seriale utilizzato per il collegamento diretto DTE-DTE, senza modem.

OSI (Open System Interconnect): standard internazionale, dell'ISO, descritto nel documento ISO 7498, per un modello di riferimento per l'interconnessione di sistemi; è organizzato in 7 livelli (Physical, Data Link, Network, Transport, Session, Presentation, Application).

OSPF (Open Shortest Path First): protocollo di tipo link state per il calcolo delle tabelle di instradamento usato nell'architettura di rete TCP/IP.

ottetto: termine OSI per indicare una stringa di 8 bit.

OUI (Organization Unique Identifier): identificativo su 3 ottetti di un'organizzazione che opera nel campo delle reti.

PABX (Private Automatic Branch eXchange): si veda PBX.

pacchetto: nome informale per una Protocol Data Unit.

packet switching o commutazione di pacchetto: tecnica di commutazione che prevede di raggruppare dati digitali in PDU e di inoltrare queste su mezzi trasmissivi condivisi dai nodi della rete.

PAD (Packet Assembler Disassembler): dispositivo utilizzato per connettere terminali asincroni a reti X.25.

PAM (Pulse Amplitude Modulation): tecnica di modulazione digitale in ampiezza.

paradiafonia: si vedano NEXT e diafonia.

parità: bit di controllo per il rilevamento di errori di trasmissione.

PBX (Private Branch eXchange): centralino telefonico ad uso privato di un ente, collegato alla rete telefonica nazionale.

PCI (Protocol Control Information): informazione di controllo del protocollo preposta alla SDU per costruire la PDU.

PCM (Pulse Code Modulation): tecnica di codifica numerica di segnali analogici utilizzata in telefonia.

PDH (Plesiochronous Digital Hierarchy): gerarchia numerica plesiocrona.

PDN (Public Data Network): termine usato per indicare le reti pubbliche per trasmissione dati.

PDU (Protocol Data Unit): pacchetto di dati trasmesso tra entità di pari livello.

piggyback: tecnica utilizzata per trasportare l'informazione di acknowledge nei pacchetti di dato.

PMA (Physical Medium Attachment): elemento di connessione fisica al mezzo trasmissivo.

polling: nei protocolli half-duplex, richiesta della stazione master ad una stazione slave per verificare se quest'ultima ha dati da trasferire.

porta: nell'architettura di rete TCP/IP, punto di accesso ai protocolli applicativi.

POTS (Plain, Ordinary Telephone Service): sigla usata per indicare la rete telefonica classica.

PPP (Point-to-Point Protocol): protocollo di livello di Data Link della famiglia HDLC per link punto-punto con capacità di multiplexing tra più protocolli di livello Network, standard in ambiente multivendor.

pps (packets per second): pacchetti al secondo, anche abbreviato p/s.

preambolo: sequenza di bit posta all'inizio di una trama per sincronizzare il clock del ricevitore.

PRI (Primary Rate Interface): interfaccia ISDN che offre 30 canali B a 64 Kb/s (in Europa, 23 canali a 56 Kb/s negli USA) e un canale D.

protocol type: campo della trama Ethernet v.2.0 indicante il protocollo di livello superiore contenuto nel campo dati.

protocollo: nell'ambito delle reti, descrizione formale del formato delle PDU e dei meccanismi di scambio delle stesse tra due entità di pari livello.

PSDN (Packet Switched Data Network): termine usato per indicare le reti a commutazione di pacchetto (in particolare quelle X.25).

pseudo nodo: nodo fittizio usato da alcuni protocolli di livello Network per evitare la presenza di tabelle di instradamento sugli ES.

PSK (Phase-Shift Keying): tecnica di modulazione di fase usata nei modem.

PSN (Packet Switched Node): nodo a commutazione di pacchetto.

PSTN (Public Switched Telephone Network): rete telefonica pubblica.

PTT (Post, Telephone, and Telegraph): agenzia governativa che gestisce le telecomunicazioni all'interno di una nazione.

PU (Physical Unit): entità utilizzata per la gestione di un nodo in una architettura SNA.

PU 2.1: la PU associata ai nodi che sono in grado di offrire LU 6.2.

QAM (Quadrature Amplitude Modulation): combinazione delle modulazioni ASK e PSK.

QoS (Quality of Service): indice della qualità del servizio nelle architetture OSI e ATM.

rapporto segnale/rumore: rapporto tra la potenza del segnale e quella del rumore in un canale, espresso in decibel.

RARP (Reverse Address Resolution Protocol): protocollo usato principalmente nell'architettura di rete TCP/IP per ottenere un indirizzo di livello Network a partire da un indirizzo di livello Data Link.

RCC (Routing Control Center): nodo centrale per il calcolo delle tabelle di instradamento, usato ad esempio nella rete Tymnet.

relay: componente elettromeccanico in cui un elettromagnete muove un insieme di contatti che chiudono ed aprono dei circuiti elettrici.

relaying: operazione di passaggio di una PDU tra due entità di pari livello all'interno di un nodo (ad esempio, nei bridge, il passaggio di una MAC PDU tra i livelli MAC di due schede di rete locale).

repeater: si veda ripetitore.

request: nel modello di riferimento OSI, primitiva di servizio attivata per richiedere la trasmissione di una PDU.

response: nel modello di riferimento OSI, primitiva di servizio dei protocolli che prevedono acknowledge attivata per indicare l'avvenuta ricezione sul nodo remoto di una PDU precedentemente trasmessa tramite una primitiva request (si veda anche confirm).

RF (Remote Fault): segnale utilizzato dallo standard 10BaseFB per segnalare un'anomalia verificatasi all'estremità opposta di un link in fibra ottica.

RFC (Request For Comments): nome di una serie di standard che trattano principalmente l'architettura di rete TCP/IP.

ring: anello.

ring purge: azzeramento dell'anello.

RIP (Routing Information Protocol): protocollo per il calcolo delle tabelle di instradamento utilizzabile per reti di piccole dimensioni.

ripetitore: unità di relaying a livello Fisico; ad esempio, nello standard IEEE 802.3, un dispositivo usato per rigenerare il segnale ed interconnettere link in cavo coassiale, fibra ottica e doppino.

ritrasmissione: tecnica utilizzata nei protocolli connessi per garantire la ricezione corretta dei dati.

round trip delay: in IEEE 802.3, parametro di progetto dipendente dalla velocità di propagazione sul mezzo trasmissivo e dalla dimensione della rete, pari al tempo necessario perché un pacchetto si propaghi da un'estremità all'altra e qualsiasi eventuale collisione raggiunga la stazione trasmittente.

route: percorso di instradamento; nei router IP esiste una route per ogni subnet raggiungibile.

router: nome informale indicante un nodo dedicato a svolgere funzionalità di IS.

routing: funzione di instradamento dei pacchetti a livello Network.

routing adattativo o dinamico: tecnica di calcolo delle tabelle di instradamento in grado di considerare dinamicamente la topologia e lo stato della rete.

routing basato sul QoS o sul COS: tecnica di instradamento che determina i cammini in funzione del tipo di servizio richiesto.

routing by network address: tecnica di instradamento utilizzata pricipalmente nei protocolli non connessi.

routing centralizzato: calcolo delle tabelle di instradamento per tutti i nodi della rete da parte di un singolo RCC centralizzato.

routing di livello 1: si veda intra-area routing.

routing di livello 2: si veda inter-area routing.

routing distribuito: tecnica di routing adattativo in cui il calcolo delle tabelle avviene tramite un algoritmo distribuito sui vari router.

routing gerarchico: tecnica di partizionamento di una rete di grandi dimensioni in sottoreti, in modo da semplificare il problema del routing suddividendolo in routing inter-area e routing intra-area.

routing statico: tecnica di instradamento in cui le tabelle sono determinate in fase di configurazione della rete.

RPC (Remote Procedure Call): estensione del meccanismo di chiamata a procedura convenzionale, che permette di attivare la procedura chiamata su un nodo remoto.

RS-232: standard per interfacce seriali, sincrone o asincrone, operanti sino a 19.200 b/s.

RUA (Received Upstream neighbor's Address): nelle reti ad anello, l'indirizzo del NAUN.

S-UTP: sinonimo di FTP.

SAP (Service Access Point): punto in cui un livello fornisce servizi al livello superiore.

SAS (Single Attachment Station): stazione FDDI che si collega al concentratore DAC tramite una sola connessione fisica, e pertanto non fault tolerant.

sbilanciata: tecnica di trasmissione di segnali elettrici con riferimento a massa.

schermatura: realizzazione di una gabbia di Faraday, da collegare a terra, attorno a un cavo o a un circuito in modo che i disturbi elettromagnetici non si propaghino dall'esterno all'interno e viceversa.

scrambling: tecnica algoritmica di ricodifica per eliminare la periodicità delle transizioni nelle sequenze di simboli da trasmettere ai fini di una riduzione delle emissioni dei disturbi elettromagnetici.

SDH (Synchronous Digital Hierarchy): denominazione europea della gerarchia numerica sincrona.

SDLC (Synchronous Data Link Control): protocollo di livello Data Link, definito da IBM per l'architettura di rete SNA, da cui è derivato l'HDLC.

SDU (Service Data Unit): unità di dati passata da un'entità a livello superiore che sta richiedendo un servizio a un'entità di livello inferiore che lo fornisce.

segmentazione: funzione in cui una SDU viene divisa in segmenti, ognuno dei quali viene trasmesso in una PDU separata.

shared LAN: LAN in cui il mezzo trasmissivo è totalmente condiviso, senza adozione di switch.

SIDL (Synchronous IDLe): segnale utilizzato dallo standard 10BaseFB per mantenere permanentemente sincronizzate le due stazioni agli estremi di un link.

Signal Quality Error (SQE): segnale di avvenuta collisione in Ethernet/IEEE 802.3.

sincrona: tipo di trasmissione dati in cui la sincronizzazione tra trasmettitore e ricevitore viene mantenuta permanentemente.

sistema: termine spesso usato, nelle reti di calcolatori, come sinonimo di nodo.

slave: nei sistemi trasmissivi punto-multipunto, una delle stazioni il cui accesso al canale è controllato dalla stazione master.

slot: unità di lunghezza fissa pari a 53 ottetti per il trasferimento dei dati nelle reti DQDB.

slot time: nelle reti CSMA/CD è la finestra di tempo necessaria per trasmettere una trama di lunghezza minima.

SMDS (Switched Multimegabit Data Service): standard per la realizzazione di reti pubblche a commutazione di cella, non connesse e ad alte prestazioni.

SMT (Station ManagemenT): funzionalità di controllo di una stazione FDDI.

SMTP (Simple Mail Transfer Protocol): nell'architettura di rete TCP/IP, il protocollo per la trasmissione dei messaggi di posta elettronica.

SNA (Systems Network Architecture): architettura di rete IBM, largamente usata sui mainframe.

SNMP (Simple Network Management Protocol): protocollo di gestione di apparati di rete appartenente all'architettura TCP/IP divenuto uno standard "de facto".

SNR (Signal to Noise Ratio) o S/N: si veda rapporto segnale/rumore.

solicitation: pacchetto inviato in broadcast per richiedere a tutti i nodi la disponibilità di un dato servizio.

SONET (Synchronous Optical NETwork): denominazione nord-americana della gerarchia numerica sincrona.

source routing: tecnica di instradamento utilizzata principalmente nelle architetture IBM e in IEEE 802.5 che consiste nello specificare in fase di generazione delle PDU la sequenza di nodi che dovranno attraversare.

spanning tree: algoritmo che riconfigura una topologia magliata di una BLAN in una topologia ad albero eliminando i percorsi alternativi, definito nello standard IEEE 802.1D.

SPF (Shortest Path First): termine spesso usato per indicare l'algoritmo di Dijkstra, in cui i cammini verso tutte le destinazioni sono calcolati a partire dal grafo della rete; utilizzato dai protocolli di routing di tipo link state packet.

SPX (Sequenced Packet eXchange): un protocollo di livello 4 utilizzato da Novell.

SQE_Test (Signal Quality Error Test): segnale trasmesso dal transceiver all'interfaccia Ethernet/IEEE 802.3 per comunicare l'avvenuto test del circuito di rilevazione delle collisioni; questo test può essere abilitato o disabilitato sul transceiver e può assumere nomi diversi come: Heartbeat o Collision Presence Test (CPT).

SSAP (Source Service Access Point): sigla usata per indicare l'indirizzo del mittente.

SSCP (Session Service Control Point): la funzionalità di gestione di un dominio in una rete SNA, normalmente realizzata dal software VTAM.

SSM (Single Segment Message): tipo di PDU nelle reti DQDB, SMDS e ATM.

stackable: tipo di ripetitore IEEE 802.3 espandibile tramite moduli collegabili esternamente.

start-stop: nome alternativo per indicare la tecnica di trasmissione asincrona il cui nome deriva dai bit di start e stop che delimitano l'inizio e la fine della trasmissione.

stazione: termine usato nelle reti locali per indicare un ES o un IS, evidenziandone le funzionalità a livello Data Link.

store and forward: metodo di commutazione in cui un pacchetto viene prima interamente ricevuto e poi ritrasmesso.

STP (Shielded Twisted Pair): cavo, normalmente a quattro coppie, avente le singole coppie schermate con fogli di alluminio ed uno schermo globale realizzato con una calza.

SUA (Stored Upstream neighbor's Address): nelle reti locali ad anello, indirizzo memorizzato relativo alla stazione NAUN.

subnet o sottorete: nell'architettura di rete TCP/IP una rete può essere suddivisa in un insieme di sottoreti mediante la definizione di una netmask.

SVC (Switched Virtual Circuit): in una NBMA utilizzante protocolli connessi, collegamento temporaneo tra due stazioni.

switch: dispositivo multiporta in grado di commutare trame a livello Data Link.

switched LAN: LAN in cui vengono utilizzati switch per aumentarne le prestazioni globali.

T1 (Trunk 1): primo livello della gerarchia PDH nord-americana con velocità di 1.5 Mb/s.

T3 (Trunk 3): terzo livello della gerarchia PDH nord-americana con velocità di 44 Mb/s.

tabella di routing: tabella contenente le informazioni utili per gli algoritmi di instradamento quali, per ogni destinazione, la linea da utilizzare, il costo e il numero di hop.

TC (Telecommunication Closet): armadio di piano secondo la nomenclatura EIA/TIA 568.

TCM (Trellis Code Modulation): tecnica di modulazione, basata sui codici di Trellis, usata nei modem.

TCP (Transmission Control Protocol): nell'architettura di rete TCP/IP, un protocollo di trasporto che offre un servizio connesso, affidabile e full-duplex, appoggiandosi di solito su IP.

TCP/IP (Transmission Control Protocol/Internet Protocol): l'architettura di rete oggi più diffusa e adottata da Internet; standard "de facto" e di mercato.

TCU (Trunk Coupling Unit): porta di connessione nei MAU IEEE 802.5.

TDM (Time Division Multiplexing): tecnica per trasmettere più canali sullo stesso mezzo trasmissivo mediante multiplazione nel tempo.

TDMA (Time Division Multiple Access): condivisione di un unico mezzo trasmissivo da parte di più canali tramite tecnica TDM.

telediafonia: si vedano FEXT e diafonia.

telnet: nell'architettura di rete TCP/IP, protocollo applicativo per la connessione interattiva ad host remoti.

terminal server: apparato di rete usato per collegare terminali seriali e stampanti ad una rete locale; normalmente utilizza i protocolli LAT e telnet.

TFTP (Trivial File Transfer Protocol): versione semplificata del protocollo FTP, utilizzata principalmente per downline loading su stazioni diskless.

throughput: misura, normalmente espressa in pps, dell'effettiva capacità trasmissiva di una rete o di un elemento di essa.

TIA (Telecommunication Industries Association): associazione di industrie di telecomunicazioni con attività nel campo della standardizzazione.

time-to-live: campo nelle PDU di livello Network utilizzato per limitarne temporalmente la vita nel caso si verificassero loop nella rete.

TO (Telecommunication Outlet): presa utente secondo la nomenclatura EIA/TIA 568 e ISO/IEC 11801.

token: particolare pacchetto la cui ricezione indica il permesso di trasmettere su un mezzo condiviso.

token passing: algoritmo di accesso ad un mezzo condiviso basato su token.

Token Ring: rete locale ad anello proposta da IBM e definita nello standard IEEE 802.5.

trama: nome generico per indicare una PDU di livello Data Link.

transceiver: nelle reti Ethernet/IEEE 802.3, dispositivo che si occupa di trasmettere e ricevere le trame sul mezzo fisico e di rilevare le collisioni.

transparent bridge: bridge di derivazione Ethernet che ha le tabelle d'instradamento a bordo ed è trasparente, nel senso che i nodi ad esso connessi ne ignorano l'esistenza.

twisted pair: si veda doppino.

UDP (User Datagram Protocol): nell'architettura di rete TCP/IP, un protocollo di livello Transport di tipo non connesso utilizzato, ad esempio, da NFS e SNMP.

UNA (Upstream Neighbor's Address): sinonimo di NAUN.

unacknowledge service o servizio non confermato: servizio in cui il richiedente non viene informato del completamento della richiesta inoltrata.

UNI (ente nazionale italiano di UNIficazione): ente italiano con attività principalmente nel settore della standardizzazione.

USART (Universal Synchronous and Asynchronous Receiver and Transmitter): dispositivo elettronico alla base della realizzazione di interfacce seriali sincrone e asincrone.

UTP (Unshielded Twisted Pair): cavo, normalmente a quattro coppie, non schermato; si veda doppino.

V.35: standard per interfacce seriali sincrone tra DTE e DCE operanti a velocità maggiori o uguali a 48 Kb/s.

VC (Virtual Circuit, Virtual Channel o Virtual Call): si veda circuito virtuale commutato.

VCI (Virtual Circuit Identifier): identificatore di circuito virtuale.

velocità di propagazione: velocità con cui un segnale elettrico o ottico si propaga attraverso un mezzo trasmissivo; espressa come percentuale della velocità della luce nel vuoto.

VPI (Virtual Path Identifier): identificatore di cammino virtuale nelle reti ATM.

VT (Virtual Terminal): applicazione di terminale virtuale remoto nell'architettura OSI.

VTAM (Virtual Telecommunication Access Method): software di gestione di un dominio in una rete SNA; realizza le funzionalità di SSCP.

WA (Work Area): posto o area di lavoro secondo la nomenclatura EIA/TIA 568 e ISO/IEC 11801.

WAN (Wide Area Network): rete che si estende su un'area geografica costruita usando servizi di telecomunicazione pubblici.

well-known port: nell'architettura di rete TCP/IP, le porte preassegnate ai principali protocolli applicativi.

X.121: standard per i piani di numerazione per le PDN.

X.25: standard CCITT per la realizzazione di reti pubbliche a commutazione di pacchetto.

X.400: nell'architettura di rete OSI, il protocollo di livello Applicativo per la posta elettronica.

X.500: standard internazionale per un servizio di nomi descrittivi in ambiente OSI, chiamato anche "directory OSI".

XDR (eXternal Data Representation): standard sviluppato da SUN Microsystem per la rappresentazione dei dati in modo indipendente dall'architettura dell'elaboratore.

XID (eXchange IDentification): tipo di pacchetto nel protocollo LLC.

XNS (Xerox Network Standard): architettura di rete definita dalla Xerox Corporation e alla base delle reti Novell.